Summer 2016

A control theoretic approach for security of cyber-physical systems

Haifeng Niu

Department: Electrical and Computer Engineering

A CONTROL THEORETIC APPROACH FOR SECURITY OF CYBER-PHYSICAL SYSTEMS

by

HAIFENG NIU

A DISSERTATION

Presented to the Faculty of the Graduate School of the

MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY

In Partial Fulfillment of the Requirements for the Degree

DOCTOR OF PHILOSOPHY

in

ELECTRICAL ENGINEERING

2016

Approved by

Jagannathan Sarangapani, Advisor

Wei Jiang

Sanjay Madria

Sahra Sedigh

Maciej Zawodniok

Al Salour

PUBLICATION DISSERTATION OPTION

This dissertation consists of the following five articles, formatted in the style used by the Missouri University of Science and Technology:

Paper I, Pages 12-62: H. Niu, E. Taqieddin, and S. Jagannathan, "EPC Gen2v2 RFID Standard Authentication and Ownership Management Protocol," IEEE Transactions on Mobile Computing, vol. 15, no. 1, pp. 137-149, 2016.

Paper II, Pages 63-104: H. Niu and S. Jagannathan, "Optimal Defense and Control of Dynamic Systems Modeled as Cyber-physical Systems," Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, vol. 12, no. 4, pp. 423-438, 2015.

Paper III, Pages 105-156: H. Niu and S. Jagannathan, "Attack Detection and Accommodation for Networked Control Systems," under review in IEEE Transactions on Control System Technology.

Paper IV, Pages 157-212: H. Niu and S. Jagannathan, "An Optimal Q-learning Approach for Attack Detection in Networked Control Systems," to be submitted.

Paper V, Pages 213-254: H. Niu and S. Jagannathan, "Attack Detection and Approximation in Nonlinear Networked Control Systems using Neural Networks," to be submitted.

ABSTRACT

In this dissertation, several novel defense methodologies for cyber-physical systems have been proposed. First, a special type of cyber-physical system, the RFID system, is considered for which a lightweight mutual authentication and ownership management protocol is proposed in order to protect the data confidentiality and integrity. Then considering the fact that the protection of the data confidentiality and integrity is insufficient to guarantee the security in cyber-physical systems, we turn to the development of a general framework for developing security schemes for cyber-physical systems wherein the cyber system states affect the physical system and vice versa. After that, we apply this general framework by selecting the traffic flow as the cyber system state and a novel attack detection scheme that is capable of capturing the abnormality in the traffic flow in those communication links due to a class of attacks has been proposed. On the other hand, an attack detection scheme that is capable of detecting both sensor and actuator attacks is proposed for the physical system in the presence of network induced delays and packet losses. Next, an attack detection scheme is proposed when the network parameters are unknown by using an optimal Q-learning approach. Finally, this attack detection and accommodation scheme has been further extended to the case where the network is modeled as a nonlinear system with unknown system dynamics.

ACKNOWLEDGMENTS

I would like to express sincere gratitude to my advisor, Professor Jagannathan Saragapani, for his close supervision, deep knowledge, patience, and general support over the last three years. I would also like to thank Dr. Maciej Zawodniok, Dr. Sahra Sedigh, Dr. Sanjay Madria, Dr. Wei Jiang, and Dr. Sriram Chellappan for serving on my doctoral committee. In particular, I would like to thank Dr. Al Salour from the Boeing Company for his support through IMS and research projects for the past four years. In addition, I would like to thank the National Science Foundation (NSF) and Intelligent System Center (ISC) for providing financial support through my Ph.D. study.

I am greatly thankful to my father, for his encouragement and also dedicate this dissertation to my beloved mother. I also would like to extend a special thanks to my girlfriend, the love of my life, Jia Cai, who has been helping and supporting me all the way along. I also express my sincere gratitude to rest of my family members back home in China for their understanding and love. I also thank all my friends here in the US and as well back home for their time and support.

Further, I would like to thank Dr. Hao Xu, who gave me many helpful discussions and suggestions concerning my work. I would like to thank my colleagues, Dr. Avimanyu Sahoo, Dr. Qiming Zhao, Lei Wang, Vignesh Narayanan, Krishnan Raghavan as well as many other friends at the Embedded Systems and Networking Laboratory, who made my Ph.D. life more fun and interesting.

Finally, I would like thank the staff of ECE department for their continuous assistance and also would like to thank the staff of Curtis Laws Wilson Library for providing me with the necessary literature.

TABLE OF CONTENTS

LIST OF FIGURES

Page

LIST OF TABLES

Page

PAPER I

PAPER II

SECTION

1. INTRODUCTION

1.1. OVERVIEW

In the past a few decades, technology, science, and engineering has significantly redefined the physical world. For example, with the new communication system such as the internet and wireless networking, we are able to interact with objects and people from almost anywhere on earth. The state-of-the-art transportation system allows us to travel to the destination within unimaginably short time. Most recently, a new class of system, named as cyber-physical system (CPS), has shown great potential of further rendering us capabilities to experience the physical world in a more secure, economical and comfortable fashion.

The CPSs are engineered systems that are constructed as networked interactions of physical and computational cyber components [1]. Applications of CPS are found in areas as diverse as automobiles, air transportation, civil infrastructure, power grid, embedded medical devices, and consumer appliances. A CPS is a highly collaborative computer system because the embedded devices monitor and control the physical processes through a networked feedback loop. A major difference between a CPS and a regular control system is the employment of communications, which adds re-configurability and scalability as well as complexity and potential insecurity. Moreover, CPS has significantly more intelligence in sensors and actuators as well as substantially stricter performance constraints [2].

Since a CPS is highly complex, spanning multiple scientific and technological domains, they thus pose several fundamental challenges, which have been summarized in [3] and presented in Figure 1.1. Six major challenges in CPS have been considered: dependability, sustainability, reliability, predictability, interoperability, and security. To be specific, dependability refers to the property of a system to perform without significant degradation in its performance whereas sustainability means the ability of renewing the system's resources and using them efficiently. Reliability refers to the degree of correctness which a system provides to perform its function while predictability refers to the degree of foreseeing of a system's behavior. On the other hand, interoperability refers to the ability of the systems to work together, exchange information and use this information to provide specified services. Finally, security in CPS, which is the main scope of this dissertation, refers to the property of a system to control access to the system resources and protect sensitive information from unauthorized disclosures.

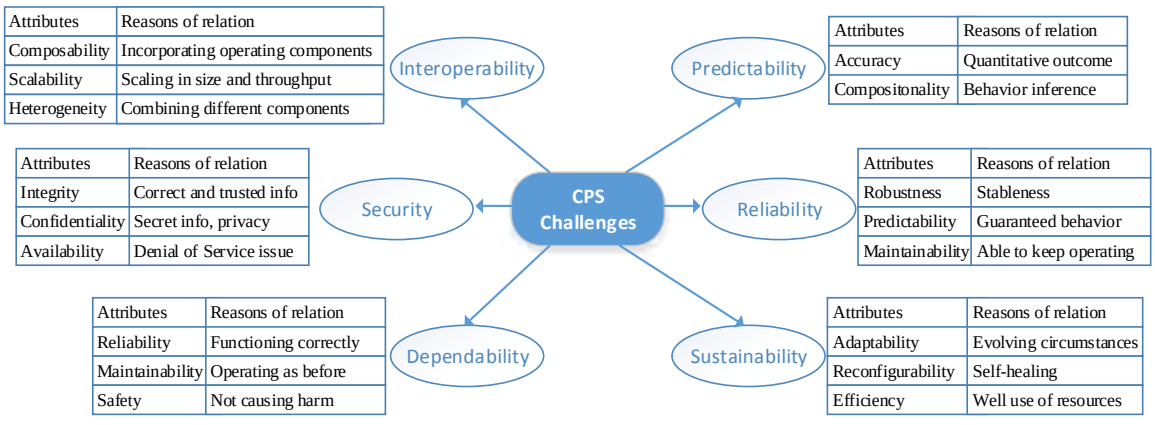


Figure 1.1. Challenges in cyber-physical systems [3].

The concern of security in CPS stems from the presence of a hierarchy of communication networks that collects information for sensing, exploring, processing and aggregating [4]. On one hand, those communication networks are often distributed over wide geographic area and thus exposed to a variety of adversaries. On the other hand, many components in CPS such as RFID sensors are low-cost embedded devices. As a result, the resources including the power budget, computational and transmission abilities are quite limited.

Therefore, the defense methodology for CPS is critical and necessary. As shown in Figure 1.2, in order to guarantee the security of CPS, the defense system is required to possess the following three capabilities: protection of information security, detection of cyber states abnormalities, and detection of physical states abnormalities.

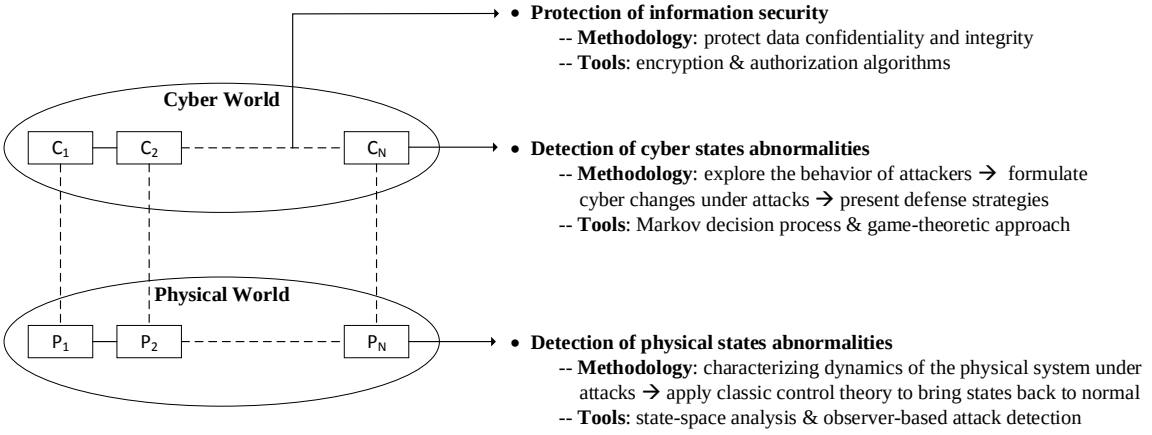


Figure 1.2. Requirements of defense methodologies for CPS.

The first requirement of the defense methodology is the ability to protect data confidentiality and integrity in the communication networks. The majority of the efforts are devoted to the development of light-weight encryption and authorization algorithms, which has been summarized in [5][6]. In particular, although RFID systems has been widely used in CPS due to their low cost and battery-free feature, the concern of disclosing the data and location privacy has not been completely addressed. The main challenge is that the computation capability of the RFID tags is too limited to implement complicated encryption algorithms and communication protocols. Due to the shared nature of wireless channels between the RFID tags and readers, various attacks can be launched by unauthorized users to either collect information about the tagged items or create a disruption of the system operation. Therefore, it is necessary for the readers and tags to authenticate each other before any data exchange. A comprehensive survey that examines several aspects related to RFID security has been presented in [7].

It is important to note that unlike the traditional information technology systems, the protection of data confidentiality and integrity alone is far from enough for CPS because certain attacks, especially those targeting at the availability of data, do not require knowledge of the cryptographic mechanisms. For example, the wormhole attacker attracts data traffic by establishing a link between two geographically distant regions of the network and then delays or drops the attracted data [8]. The jamming attacks over wireless networks may severely degrade the performance in terms of message delay and data throughput by broadcasting radio interferences [9]. The replay attacker maliciously repeats the messages delivered from the operator to the actuator and causes communication unreliability, which has been successfully used by the virus attack of Stuxnet [10][11]. This

explains the necessity for the defense methodology to meet the second requirement introduced in Figure 1.2.

The second requirement of the defense methodology is the ability to detect the cyber state abnormalities. In order to meet this, the defender needs to explore the behavior of the attackers, formulate the cyber changes under attacks, and present an appropriate strategy to bring the cyber system back to normal. For instance, the effort in [12] introduces the DoS flooding attacks by a continuous-time Markov chain and utilizes the state space method to compute security measures accurately. Different from [12], the authors in [13] study the cyber defense by modeling the actions of the attacker and the defender as a stochastic zero-sum game. In [14], the measure of vulnerabilities in cyber-physical systems with application to power systems is defined and a security framework including anomaly detection and mitigation strategies is provided. The authors in [15] evaluate the cyber security by computing the expected probabilities of the attacker and using the probabilities to build a transition model through game-theoretic approach. In [15], the cyber vulnerability is evaluated dynamically by using hidden Markov model and by providing a mechanism for handling sensor data with different trustworthiness.

In particular, selecting the network traffic flow as the cyber states provides a feasible to way to deal with the previously mentioned cyber-attacks [8-11] since it is observed that these attacks tend to deviate the amount of traffic flow from the normal value. Flow control has been studied in the literature [16-18]. For example, the authors in [16] model the high-speed network as fluid-flow queues with a fixed propagation delay for each channel. In [17], a receiver-based flow control scheme is proposed that achieves the given optimal utility. The authors in [18] propose a new utility max-min flow control framework

using classic sliding mode control. However, to the best of our knowledge, minimal effort has been spent on studying the flow control from the perspective of network security when the network is attacked by injecting or dropping traffic flow.

The third requirement of the defense methodology is the ability to detect the state abnormalities of the physical system. This can be done through characterizing the dynamics of the physical system under attacks by extending the classical state-space description. For instance, in [20], the system dynamics include an extra term to model the deception attack. In [21], the system state under attack is represented with an additive term which in turn is used to simulate the false data injection attack. The authors in [22] characterize the deception attacks using a set of objectives and propose policies to synthesize stealthy deception attacks. In [23], the estimation and control of linear systems when sensors or actuators are corrupted by an attacker is provided, together with a secure local control loop that can improve the resilience of the system.

However, there are many weaknesses in the reported work [12-15][20-23]. First of all, these approaches only focus on either the cyber system or the physical system and fail to take the interactions between the cyber defense policy and the system controller performance into consideration. Second, the representations [8-11] can only describe a single type of attack due to the fact that attacks affect the system dynamics in a variety of ways. Last but not least, it is difficult to implement the representation developed in the literature so far since the system dynamics under attacks are considered known. For instance, the physical system dynamics becomes uncertain due to random delays and packet losses caused by certain cyber-attacks [24].

To conclude, in order to guarantee the security of CPS, the defense methodology is required to be capable of protecting the information security and detecting cyber state abnormalities as well as the physical state vector abnormalities. Such a comprehensive defense framework, which is lacking in the existing literature to the best of our knowledge, is the main objective of this dissertation.

1.2. ORGANIZATION OF THE DISSERTATION

In this dissertation, a comprehensive defense framework and several novel defense methodologies for CPS has been proposed. This dissertation is presented in five papers, and their relationship to one another is illustrated in Figure 1.3. The common theme in these five papers is the development of defense methodologies for cyber-physical systems.

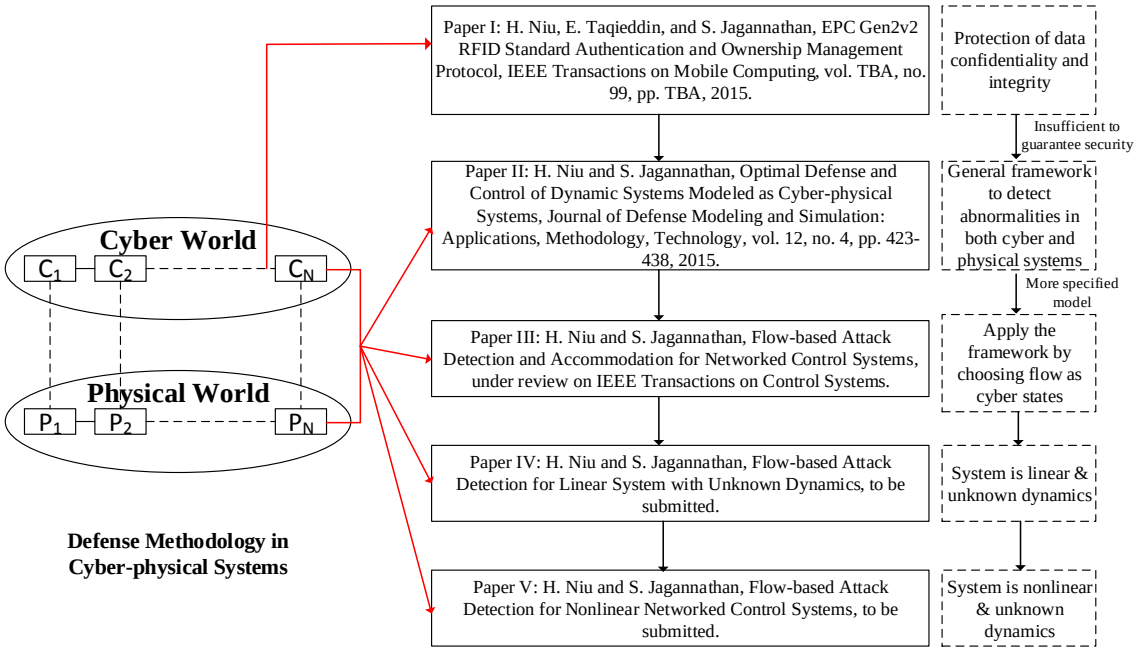


Figure 1.3. Dissertation outline.

In the first paper, the objective is to protect data confidentiality and integrity for a particular cyber-physical system – mainly in RFID systems. To this end, a lightweight mutual authentication and ownership management protocol is proposed. The protocol is compliant with the latest EPC Gen2v2 standard. The protocol is designed to fit within the computational abilities of the tag as well as the scarce energy resources. The details of the protocol are given along with formal security proof of its correctness. Further, the protocol is implemented on EPC compliant tags and is shown to add minimal overhead to the standard message exchanges.

Next, since the protection of the data confidentiality and integrity is insufficient to guarantee the security in CPS, in the second paper, we propose a novel representation for developing security schemes wherein the cyber system states affect the physical system and vice versa. Subsequently by using this representation, an optimal strategy via Q-learning is derived for the cyber defense in the presence of an attack. Since the cyber system under attack will affect the physical system stability and performance, an optimal controller by using Q-learning is considered for the physical system with uncertain dynamics. As an example, cyber-attacks that increase the network delay and packet losses are considered and the goal of the proposed cyber defense and optimal controller is to thwart the attack and mitigate the performance degradation of the physical system due to increased delays and packet losses.

In the third paper, we further apply the framework proposed in the second paper by selecting the traffic flow as the cyber system states. To be specific, we first propose a novel attack detection scheme that is capable of capturing the abnormal traffic flow in the communication links due to a class of attacks. Further, it is shown that the stability of the

physical system can be affected by the condition of the network due to delays and packet losses induced by the attacks. An observer-based detection scheme is developed both for the network and physical system. Attacks on the networks as well as on the physical system can be detected and upon detection, the physical system can be stabilized by adjusting the controller gains. Several attacks are considered in the simulation to show the applicability of the proposed scheme.

Subsequently, in the fourth paper, the work in the third paper is extended to the case where the CPS dynamics becomes unknown due to the unknown network parameters. Accordingly, an adaptive observer is proposed to estimate the unknown system dynamics and an optimal Q-learning based controller is developed to stabilize the flow in the presence of disturbances. The detection residual generated by the adaptive observer is in turn utilized to determine the onset of an attack when it exceeds a predefined threshold. For the physical system, we consider a stochastic dynamic system which incorporates uncertain network-induced delays and packet losses in the system dynamics. The proposed detection scheme includes an optimal Q-learning based event-triggered controller that is capable of detecting attacks on both sensors and actuators.

Finally, the last paper considers the case where the network traffic flow is modeled as a nonlinear system with unknown dynamics. A one-layer neural network (NN) based estimator is adopted in order to approximate the unknown system dynamics. Similar to Paper IV, the network attack detection residual generated by the adaptive observer is utilized to determine the onset of an attack. Upon detecting the attack, another NN-base approximator is introduced to estimate the attack input. For the physical system, we develop an attack detection scheme by using an optimal or approximate dynamic

programming-based event-triggered controller in the presence of network delays and packet losses. Moreover, attacks on the sensor or actuators of the physical system can be detected and further estimated with the proposed attack detection scheme.

1.3. CONTRIBUTIONS OF THE DISSERTATION

This dissertation provides contributions to the area of defense methodologies for the cyber-physical systems. The proposed uniform representation for CPS can be used in a variety of applications including autonomous systems. In particular, the cyber defender is able to make thorough decisions by selecting appropriate cyber state vector and output and customizing the payoff function that is of interest. Therefore, the proposed effort overcomes these deficiencies mentioned in Section 1.1.

The contributions of Paper I include the development of a novel lightweight authentication and ownership transfer protocol for passive RFID systems. We also demonstrate how the proposed protocol is compliant with the EPC Gen2v2 standard. The protocol is analyzed by using strand space and implemented and evaluated on hardware, which, to the best knowledge of the authors, is the first hardware based evaluation for ownership transfer protocols.

For the second paper, the main contribution is the novel and comprehensive representation of the CPS that captures the interrelationship between the cyber and the physical elements. The optimal strategies for the defender and the attacker are also developed based on the proposed framework.

On the other hand, the contributions of the third paper include the design of the flow controller with randomly delayed measurement in the presence of attacks and the development of novel observer-based network attack detection and estimation scheme

along with detectability condition. A controller is also designed for the physical system to maintain the stability of the physical system which can be utilized to maintain the healthy condition of the communication networks in terms of the delays and packet losses using adversary models.

The contributions of the fourth paper include the design of the optimal flow controller in the presence of disturbances and cyber-attacks, where the network parameters are considered unknown. A novel observer-based network attack detection and estimation scheme along with detectability condition is also provided. The contribution of the fourth paper also includes the development of sensor/actuator attack detection scheme with an event-triggered controller for the physical system with uncertain system dynamics.

Finally, for the last paper, the main contributions include the development of a novel observer-based network attack detection and estimation scheme for nonlinear NCS with unknown system dynamics. It is demonstrated that the proposed scheme works in the presence of a class of attacks with specific adversary models. The contributions on the physical system include the development of an event-triggered controller in the presence of network-induced delays and packet losses and a sensor/actuator attack detection and estimation scheme.

PAPER

I. EPC GEN2V2 RFID STANDARD AUTHENTICATION AND OWNERSHIP MANAGEMENT PROTOCOL

Haifeng Niu, Eyad Taqieddin, and S. Jagannathan

Providing security in passive RFID systems has gained significant attention due to their widespread use. Research has focused on providing both location and data privacy through mutual authentication between the readers and tags. In such systems, each party is responsible of verifying the identity of the other party with whom it is communicating. For such a task to succeed, the tags and readers are initialized with shared secret information which is updated after a successful authentication session. Ownership management, which includes transfer and delegation, builds upon mutual authentication. Here, the use of security in RFID is extended to encompass the more practical case where a tagged item is shifted from one owner to another. As such, we propose a new authentication and ownership management protocol that is compliant with the EPC Class-1 Generation-2 Version 2 standard. The protocol is formally analyzed and successfully implemented on hardware. The implementation shows that the use of such protocol adds security with little added overhead in terms of communication and computation.

1. INTRODUCTION

Radio Frequency Identification (RFID) systems are deployed in numerous automated asset management applications. Examples of such applications include libraries, warehouses, and border control to name a few. In a RFID system, the identification information of the tracked objects is stored in a nonvolatile memory on passive tags. These tags are queried by readers which transmit an RF signal to energize the tags so as to get the backscattered information. The readers are connected to backend servers which store and process the data.

An important aspect to be considered in RFID systems is the data and location privacy. Given that the communication between the tags and readers is wireless, various attacks may be launched by an unauthorized user to either collect information about the tagged items or cause a disruption of the system operation. As a result, the communicating parties, a tag and a reader, must authenticate each other before any data exchange. Moreover, the data should be concealed from unauthorized access through encryption. As such, both the reader and the tag need to share secret information.

Besides authentication, ownership management (i.e.; transfer or delegation) (OT) is also an important aspect of RFID security as most tagged items will change owners at least once during their lifetime. For example, the ownership of the tagged item is transferred from the manufacture to the retailer, and then to the customer. Special attention to the security must be paid because this process is relatively vulnerable to attacks due to the exchange of secret keys or passwords. Further, it is desired that the ownership management protocol would protect the privacy of the new owner from tracking by the

previous owner(s) and to guarantee that the new owner will not be able to retrieve the previous secret keys used by the old owner.

To add security features to the passive tags, the EPC Class-1 Generation-2 standard (EPC Gen2v1) [1] introduces the access and kill password. The access password is used whenever the reader wishes to read/write data in a tag's memory. On the other hand, the kill password along with the kill command is issued to stop the tag from responding to any subsequent queries. These basic security mechanisms are easily defeated because the passwords are XORed with a random number that is sent in plaintext, which can easily be retrieved.

Recently, the EPC Class-1 Generation-2 standard version 2 (EPC Gen2v2) [2], has been ratified. Backward-compatible with the old version, the new one provides a series of features intended to improve security of the tag by allowing the manufacturers to customize the cryptographic authentication methods to verify identity and provenance, as well as avoid unauthorized access. Similar to the previous standard, EPC Gen2v2 supports the use of a pseudo random number generator (PRNG), a cyclic redundancy check (CRC) function, and XOR operation.

A security protocol is usually considered as "EPC compliant" if it solely uses one or more of these functions. However, these functions by themselves are not cryptographic functions. Other measures should be taken to provide an acceptable level of security considering their computational capabilities since there are only 500 – 5000 gate elements on the tag, of which 200 – 2000 can be used for security-related functions [3]. The Advanced Encryption Standard (AES), for example, requires about 3000 gate elements to be implemented. Hash functions like MD5 and SHA-256 require even more gate elements,

8000 – 10000 [4]. Therefore, securing information among RFID devices is a major challenge due to the limited storage and computational capabilities on the passive tags.

1.1. RELATED WORK

A comprehensive survey [5] examines several aspects related to RFID security. Mainly, the importance of mutual authentication and secret information sharing is emphasized. In [6], a classification of RFID authentication protocols, based on the cryptographic/logical functions, is presented. These protocols range from full-fledged protocols in which symmetric, asymmetric, and hash functions are supported [7]-[12] to the least computationally demanding class called the ultra-lightweight, where basic bitwise logical and shift operations are employed [13]-[16].

In [17], an EPC compliant mutual authentication protocol based on CRC exchange followed by update on secret information after each authentication session is proposed to provide privacy, anonymity, and to resist replay and denial of service (DoS) attacks. However, [18] and [19] indicated that [17] did not achieve its intended goals. The work of [18] detailed the steps to successfully impersonate a valid tag either temporarily or permanently and how to run a DoS attack. These attacks are shown to be practical due to the short length of the data units exchanged. In [19], the impersonation attack is extended to include the back-end database as well as the tags. The analysis shows how the location of the tag can be identified and tracked.

The authors in [20] proposed a new protocol called Azumi to overcome the security flaws of [21] and claim that it is capable of defending against location tracking, DoS attacks, counterfeit reader or tag, and man-in-the-middle (MitM) attacks. However, it is

shown that the work in [20] is vulnerable to tag impersonation and secret disclosure attacks. An enhanced version Azumi+ was proposed in [22] as a solution.

Several research efforts considered the problem of ownership management. One of the earliest ownership transfer protocols appeared in [23]. However, the old owner privacy cannot be guaranteed due to the way the shared keys are updated, leading to a de-synchronization attack. Around the same time, the authors in [24] proposed a scalable, delegated pseudonym protocol enabling ownership transfer. However, as pointed out in [25], the keys shared by several tags become a weakness that reduces security. In [26], a protocol based on the use of hash functions, symmetric cryptography, and the XOR operation is proposed. The protocol is shown to be vulnerable to tracking and DoS attacks by manipulating the value of the random number sent to the tag [27]. Moreover, in [28], an attacker can add noise to the final message exchange resulting in the tag holding incorrect secret information due to which any subsequent authentication would fail.

Another protocol appeared in [29] referred to as product-flow ownership-transfer protocol (POP). This protocol supports querying, disabling, or updating the secret keys on the tag. However, this protocol does not provide privacy to the new owner because the old owner will still be able to access the tag by exploiting his knowledge of the shared secret keys. In addition, it is prone to de-synchronization attacks similar to [30], [31].

As for ownership delegation protocols, for example, the work in [30] assumes that the channel from the tag to the reader is secure and that any ownership transfer/delegation will be securely accomplished. This is an impractical assumption and cannot be relied upon. Another variant of [26] was proposed in [33] as an ownership delegation protocol. Delegation is possible because the message containing the new key uses the old key as a

variable. As such, the old owner will be able to keep track of the key updates and modify its keys accordingly.

The ownership management protocols mentioned above [23]-[30], as well as in [32]-[35], are not EPC compliant due to the nature of the cryptographic functions used in computing the messages. An EPC compliant lightweight protocol is given in [36] wherein PRNG and XOR functions are used on the tag side. However, the protocol is sensitive to replay and MitM attacks. Another EPC compliant ownership transfer protocol is proposed in [37] where the authors add a modular division operation to the functions of the tag because such a function would not require a large number of gate elements. However, a potential attacker can disguise as an owner who can update the secret keys in the same way as the new owner does, thus eliminating the security.

The other ownership transfer protocols [37]-[41] conforming to EPC standards use CRC as the encryption method and cannot guarantee security because of the complete linearity property of CRC. In fact, as analyzed in [19] and [39][42], the attacker is able to trace, impersonate and eventually disclose all the information stored in tags with very few interactions. In summary, an EPC compliant secure authentication and owner management protocol is yet to be developed for passive tags.

1.2. CONTRIBUTIONS

In this paper, a lightweight mutual authentication and ownership management protocol is proposed. The protocol is compliant with the EPC Gen2v2 standard. The basic supported operations, along with permutation, are used as basic operations to provide the cryptographic functionality.

The protocol is designed to fit within the computational abilities of the tag as well as the scarce energy resources. The details of the protocol are given along with formal security proof of its correctness. Further, the protocol is implemented by using EPC compliant tags and is shown to add minimal overhead to the standard message exchanges. This paper is an extended version of work published in [43]. We extend our previous work by making the following improvements. 1) In addition to the basic ownership transfer scheme introduced in [43], the protocol presented in this work also supports ownership delegation. 2) A mathematical proof of both authentication and secrecy with strand space theory is provided. 3) A detailed description on how the proposed protocol is implemented in hardware is offered. 4) More experiments are conducted to evaluate the performance of the proposed protocol, such as time consumption analysis for multiple-tag ownership transfer and resistance evaluation to the brutal force attack.

The main contributions of this work include: 1) the development of a novel lightweight authentication and ownership transfer protocol for passive RFID systems by taking into account both delegation and ownership transfer into consideration, 2) the demonstration of how the proposed protocol is compliant with the EPC Gen2v2 standard, 3) the security analysis of the protocol by using strand space, and 4) hardware implementation and evaluation, which, to the best knowledge of the authors, is the first hardware based evaluation for ownership transfer protocols.

The rest of the paper is organized as follows. In Section 2, the detailed description of proposed protocol is given followed by the security analysis given in Section 3 and a comparison with pervious work in Section 4. The hardware implementation and evaluation is given in Section 5. The paper is concluded in Section 6.

2. PROPOSED PROTOCOL

In addition to the limited functions supported by the EPC standard, the available power on the tag for various computations and transmissions needed as part of the security protocol implementation is an important constraint. Moreover, the limited available time for executing the steps for the authentication and ownership management protocol is an added challenge. Finally, the protocol has to be implemented in a practical setting in which hundreds or thousands of tags are present with several tags simultaneously performing exchange and this should be completed within the allowed timeslot.

To enhance the functionality of the protocol, the ultra-lightweight permutation operation (Per) [16] is added to the existing functions on the tag. This operation offers diffusion of the bits and helps overcome any problem occurring because of the nature of bitwise operations. The operation is defined as follows:

Definition 1 [16]: For two n-bit strings, X and Y, in the form

$$X = x_1 x_2 \cdots x_n,\ x_i \in \{0,1\},\ i = 1,2,...n;\ Y = y_1 y_2 \cdots y_n,\ \mathrm{y}_i \in \{0,1\},\ i = 1,2,...n.$$

The Hamming weight of Y, $wt(Y)$, is m $(0 \le m \le n)$ and

$$y_{k_1} = y_{k_2} = \cdots = y_{k_m} = 1,\ y_{k_{m+1}} = y_{k_{m+2}} = \cdots = y_{k_n} = 0,$$

where

$$1 \le k_1 < k_2 < \cdots < k_m \le n,\ 1 \le k_{m+1} < k_{m+2} < \cdots < k_n \le n.$$

Then, the permutation of X according to Y, denoted as $Per(X,Y)$, is given by

$$Per(X,Y) = x_{k_1} x_{k_2} \cdots x_{k_m} x_{k_n} x_{k_{n-1}} \cdots x_{k_{m+2}} x_{k_{m+1}}.$$

The following assumptions are made in designing the protocol:

1) The link between the readers is secure. Also, the link between any reader and the trusted third party (TTP) is assumed to be secure. This is a reasonable and quite common assumption as the readers are built with more powerful processors which can take advantage of complex encryption algorithms to guarantee secure data transmission.
2) The link between the tag and any other entity is considered insecure.
3) The current owner and the tag share a secret key that is only known to them.

2.1. INITIALIZATION

The tag is initialized with the following values:

1) K: secret key shared with both current and new owners, as well as delegates, if any.
2) K_M: master key only shared with the tag owner. A reader with K_M is able to modify key K, but a reader with key K does not have access to K_M.
3) K_{TTP}: key shared between the tag and the TTP.
4) EPC: electronic product code, the static identifier of a tag.
5) R_{IDi}: The ID of the reader *i* currently owning the tag.
6) IDS: In the protocol, index pseudonym (IDS) is exchanged instead of using the tag identifier (ID). The IDS is a pointer to a database entry in which the information of the tag is stored. Such an entry may include the identifying information and the keys related to that tag. We use the IDS instead of concealing the EPC in the messages, for the following two reasons: 1) The EPC value is constant and its use in multiple runs of the protocol may reveal information about the tag and its secret values. 2) Tracking the EPC by the old owner is possible.

Note that for compliance with the EPC standard, all data units in the protocol are 96 bits long. For the convenience of implementation, these 96-bit data are broken into six 16-bit words. For example, a 96-bit parameter A is broken into six words, denoted as $A(1), A(2), ...A(i), ...A(6)$, where $A(i)$ is the *ith* 16-bit subunit. As a result, all the computations are executed six times in order to get the complete 96-bit data.

The current owner is initialized with K, K_M, IDS, R_{IDi} and EPC. As mentioned earlier, the proposed ownership management protocol takes both delegation (details in Section 2.3) and complete ownership transfer (Section 2.4) into consideration. However, it is important to notice that before either delegation or complete ownership transfer take place, mutual authentication is needed to verify the authority of all parties involved.

2.2. PHASE I: MUTUAL AUTHENTICATION

A general scenario for an authentication session starts with the reader querying a tag. In response, the tag sends an index pseudonym (IDS). A sequence of exchanges follows such that the reader securely sends random numbers to the tag by using the shared key, the tag authenticates the reader and vice versa, and the keys and IDS are updated. The transactions that take place are shown in Figure 2.1.

The purpose of the authentication phase is to: 1) prove the possession of shared secret key to each other without disclosing it; 2) pass the nonces that are used to update the keys. To achieve this, the reader generates two 96-bit random values (rnd1, rnd2) as the nonces, then computes A, B, and C in a way described in Figure 2.1. Particularly, in the computation of A and B, the secret key is part of the input of PRNG function so that the key is protected while the tag can verify the readers' possession of the key by doing the same computation. Furthermore, message C is used to check if the tag has retrieved the

correct nonces (rnd1, rnd2) from messages A and B. It is very important to note that the PRNG is a nonlinear function, meaning that if an attacker flips one bit of RID2, the tag will get a totally different (and incorrect) rnd1. Moreover, since rnd1 is used to retrieve rnd2 from B, therefore rnd2 derived by the tag will be incorrect, As a result, even if the attacker flips the same bit of B, it will not get C' that equals to C.

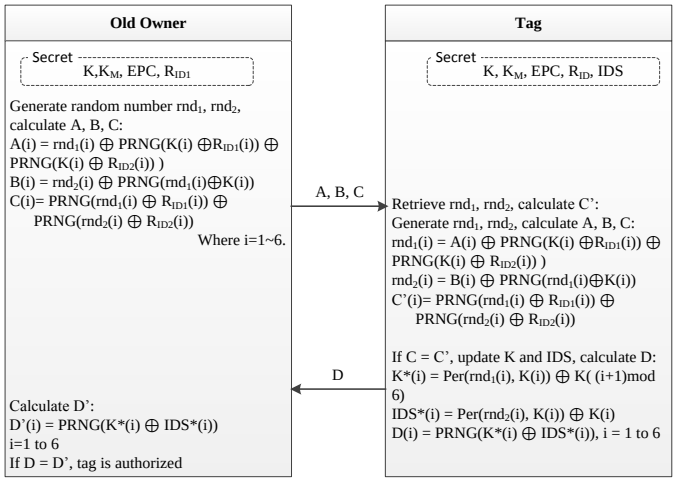


Figure 2.1. Mutual authentication and keys update [43].

If C equals to C', then it is believed that the reader does have the secret key and the tag has retrieved rnd1 and rnd2 successfully. Then the new key and IDS are computed in a way specified in Figure 2.1. Similarly, we use message D to: 1) prove the tags' possession of the secret key; 2) inform the reader that the tag has computed the new key and IDS.

Upon receiving message D, the reader will compute D' in the same manner and determines whether D equals to D' or not. If that is true, then the tag is authenticated. Consequently, the reader and the tag update to the new computed key and IDS for future uses. It should be noted, however, that both the reader and the tag should maintain a copy of the old key and IDS to avoid desynchronization problems (more explanation can be found in Section 4).

2.3. PHASE II, CASE 1: DELEGATION

At this point, RID1 is ready to delegate its rights over the tag to RID2. For that purpose, we introduce the use of the ticket. This is used by the delegate reader to prove to the tag that it is a valid reader and that it had received sufficient credentials from the current owner to allow it to access the tag. In the proposed delegation protocol, both RID1 and the tag compute the ticket as shown in Figure 2.2.

Figure 2.2. Ticket computation on an old owner and tag.

RID1 uses a secure link with RID2 and passes to it the EPC, IDS, K, and ticket. A valid ticket allows RID2 to query the tag and to run mutual authentication sessions with it.

Figure 2.3 shows how the delegate RID2 uses the ticket to query and update the tag. Note that the ticket value becomes an integral part of the message computations.

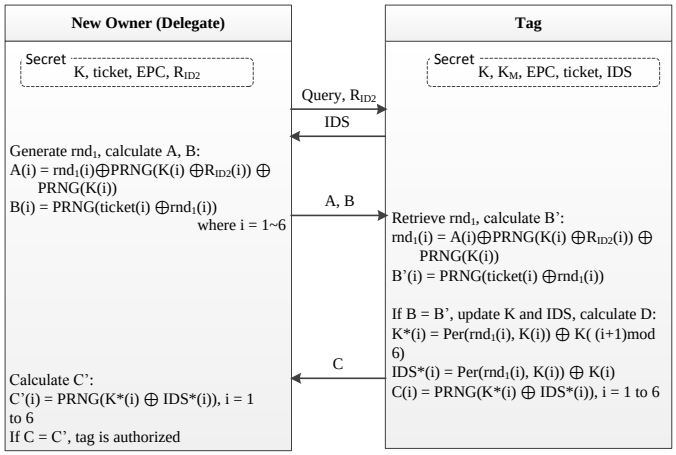


Figure 2.3. Ownership delegation.

In the case of delegation, RID1 may wish to restore its sole ownership of the tag. This means that it has to revoke the ticket such that RID2 will not pass the test of equality between B and B'. When that happens, no update will take place and the tag will not run further session with the revoked reader. The proposed approach for this is to modify the value of K_M such that the ticket given to RID2 will not match with the computed value. Note that the value of the ticket is updated with every session because the values of rnd1 and rnd2 are changed.

Delegation is suitable for those cases where certain “guest readers” need to access the tag temporally. In other cases, however, the old owner needs to give up the ownership completely and transfer it to the new owner. This process is presented in the following section.

2.4. PHASE II, CASE 2: COMPLETE OWNERSHIP TRANSFER

In this case, we propose the use of a TTP to guarantee the correctness of the protocol. The need for the TTP arises from the fact that the old owner holds the same values shared between the new owner and the tag. This means that any update taking place by RID2 may be mirrored by RID1. This violates an important property of ownership transfer which is backward privacy.

However, it is worth to note that the EPC Gen2v2 standard introduces a new “untraceable” command, which allows the tag to reduce its operating range for all readers. This function, to some degree, may give a practical solution of releasing the use of TTP by reducing the operating range so that only the new owner can reach the tag. As a result, the old owner cannot repeat the key update process and thus the backward privacy is guaranteed.

In this protocol, the goal is to change the value of K_M stored on the tag such that it matches that stored on RID2. After that, RID1 will have no access to the tag anymore. This proposed approach adds an extra functionality that we may use the reverse process in case we wish to satisfy the ownership repossession property. As presented in Figure 2.4, the outline of the protocol includes those steps:

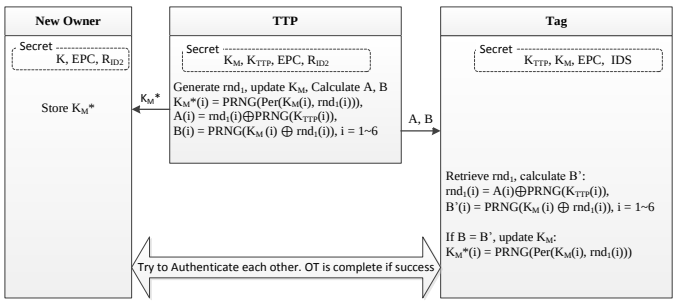


Figure 2.4. Complete ownership transfer [43].

1) TTP generates a random number rnd_1 and uses it to update K_M to K_M^*. This will become the new master key shared between the tag and the new owner, RID2.
2) TTP sends K_M^* to RID2 using the secure channel.
3) The challenging part for the TTP becomes to send K_M^* to the tag. For that, we propose the use of messages A and B shown in Figure 2.4. Similar to what we have done in the authentication phase, the secret key is set as the input of the nonlinear PRNG function while the nonce is XORed with the PRNG output so that the key will not be disclosed and the nonce can be passed to the tag safely. Message B is used for the tag to verify TTP's possession of the secret key and to check the correctness of the nonce.
4) The tag retrieves $rnd1$ from A and verifies that B is equal to B'.
5) The value of rnd_1 is used by the tag to update K_M^* in a manner similar to that used by the TTP.
6) The new owner and tag need to challenge each other to verify that both have the same value of K_M^*.

2.5. EXAMPLE OF AUTHENTICATION AND OWNERSHIP TRANSFER

To illustrate the operations that take place, we give a numeric example. Assume that the tag is initialized with the following values:

K = 0xF702A7DE0826C3F829A1E411;

KM = 0x5998C1D7782AB07071536E71;

KTTP = 0xD4B087E2874D2702DE62DE89;

RID1 = 0x8C00CACD2BD37051AE008186;

RID2 = 0xF51EF5A0B4BF61ADA7B4B2F6.

According the protocol, the reader generates two random numbers to be used in the computation of messages A, B, and C. Assuming that the random numbers are

rnd1 = 0x18F86BF86469F341C132C052;

rnd2 = 0x474BEA6DA7CD08D146A9414E.

The reader will then send

A = 0xC8D9BBBC295F1707A0D1B9D7;

B = 0xB2430574BF1375B0B3186233;

C = 0xB09F6C3B632DD765C2F767D4.

Upon receipt of these values, the tag retrieves rnd1 and rnd2 from messages A and B, and then computes C’ to compare it with C. If they match then the tag computes new values for K and IDS and uses these updated values to compute D.

K* = 0xB7E16E19AB54DF2527093616;

IDS* = 0xB8A64333A6C0C36F650BA775;

D = 0x2453BE3D512DB598394CD738.

The reader verifies the value of D by comparing with D'. If they match then the tag and reader both have successfully authenticated each other and updated their secret key and IDS values.

The ownership transfer phase follows a similar manner. Messages A and B are used between the TTP and the tag to convey a random number and to prove to the tag that the messages originate from an authentic source, the TTP. To illustrate, assume that the TTP generates rnd1 as

$$rnd1 = 0x411895D3C7772A68D368159E.$$

Then A and B will be

$$A = 0x330B34429236E6B83E1BD20C;$$

$$B = 0x4DC01DE6C69F8F6E88E025D0.$$

The tag retrieves rnd1 and then updates KM to

$$KM^* = 0x232F1EBB84FED34E175A0797.$$

The same key is already in the possession of the new owner through the secure channel with the TTP. Thus, the tag and the new owner can communicate with each securely using the new key. Note that the old owner will not be able to compute KM* since it does not have the rnd1 value.

3. SECURITY ANALYSIS

In this part, we use the strand space analysis to prove the correctness of the protocol. A strand is a sequence of events that a single principal may engage in, while a strand space is a set of strands [44]. Here, "principal" stands for any participant that may be involved in the protocol such as old/new owner, tag, attacker, or TTP [44]. In the following analysis, we use some of the definitions and lemmas provided in [44]. We analyze the security of the authentication phase only. The analysis of the other two phases is either part of or identical to that of the authentication phase.

Let T_{name} $\mathrm{T_{name}}$ be the set of names such as R_{ID1} and R_{ID2} $\mathrm{R_{ID1}}, \mathrm{R_{ID2}}$, and IDS IDS Key $\mathrm{Key_x}$ is the set of keys known by the principal x. Let m be a message and K is a key, then we represent the encryption of message m using K as $\{m\}_k$ $\{\mathrm{m}\}_\mathrm{K}$. Also, K^{-1} is the corresponding decryption key of K. Now, for simplicity, we rewrite messages A, B, C and D:

$$A = rnd_1 \oplus \{K, R_{ID1}\}_{K_{A1}} \oplus \{K, R_{ID2}\}_{K_{A2}}; \quad (1)$$

$$B = rnd_2 \oplus \{K, rnd1\}_{K_B}; \quad (2)$$

$$C = \{rnd1, R_{ID1}\}_{K_{C1}} \oplus \{rnd2, R_{ID2}\}_{K_{C2}}; \quad (3)$$

$$D = \{K^*, IDS^*\}_{K_D}, \quad (4)$$

where $K_{A1}{}^{-1}, K_{A2}{}^{-1}, K_B{}^{-1}, K_{C1}{}^{-1}, K_{C2}{}^{-1}$ and $K_D{}^{-1}$ are unknown to all the principals because of the one-way property of PRNG function. We can show that under the following Assumption 1, this presentation is equivalent to the original one in Figure 2.1 in the sense of security.

Assumption 1: If $y = PRNG(x)$ and y is known to a principal P, then the probability that P is able to compute the value of x is negligible.

According to EPC Gen2v2 standards [2], the PRNG function shall meet the following randomness criteria:

1) The probability P that any RN16 has value $RN16 = j$, for any j, should be bounded by $0.8/2^{16} < P < 1.25/2^{16}$.
2) For a tag population of up to 10,000 tags, the probability that any two or more tags simultaneously generate the same sequence of RN16s shall be less than 0.1%.
3) An RN16 drawn from a Tag's PRNG 10ms after the rise time shall not be predictable with a probability greater than 0.025% if the outcomes of prior draws from the PRNG, performed under identical conditions, are known.

In our protocol, the 96-bit random number consisting of six 16-bit random numbers is used which means that the probabilities defined in the above criteria are much smaller (new probability P' equals to P^6, not just $6P$). Therefore, this assumption is reasonable. Taking the computation of message A as an example, we can conclude that even if a penetrator managed to get the value of both $PRNG(K \oplus R_{ID1})$ and $PRNG(K \oplus R_{ID2})$ (in fact he can only know the XOR results of them), by Assumption 1, he still cannot compute the value of K, R_{ID1} and R_{ID2}.

Next, we will introduce the definition of the proposed ownership transfer strand space S_{OT}.

Definition 2: An infiltrated strand space Σ, P is an S_{OT} space if it is the union of three kinds of strands:

1) Penetrator strands $s \in \mathrm{P}$, the set of keys known by P is Key_P ;

2) "Initiator strands" $s \in Init[K, rnd1, rnd2, R_{ID1}, R_{ID2}]$ with trace:

$$< +\{R_{ID1} R_{ID2}\}, -\{IDS\}, +\{ABC\}, -D >,$$

where $A, B, C,$ and D are defined in (1) to (4) and the sign "+" means sending out a message while "-" means receiving. The principal associated with this strand is the old owner. We will use $Init[\cdot]$ to denote the set of all the strands shown above. The set of keys known by Init is Key_I.

3) Complementary "responder strands" $s \in Resp[K, rnd1, rnd2, R_{ID1}, R_{ID2}]$ with trace:

$$< -\{R_{ID1} R_{ID2}\}, +\{IDS\}, -\{ABC\}, +D >.$$

The principal associated with this strand is the tag. Similarly we will use $Resp[\cdot]$ to denote the set of all the strands shown above. The set of keys known by Resp is Key_R.

Figure 3.1 shows the strand space representation of the proposed ownership transfer protocol. In the next two parts, we prove the two aspects of correctness respectively: authentication and secrecy.

3.1. AUTHENTICATION

In [45], G. Lowe introduces four reasonable meanings of the word "authentication." They are, from the weakest to the strongest, aliveness, weak agreement, Non-injective agreement and agreement. In this paper, we prove that the proposed protocol satisfies the strongest definition: agreement.

Definition 3 (Agreement [45]): A protocol guarantees to an initiator A agreement with a responder B on a set of data items if, whenever A completes a run of the protocol,

apparently with B, which apparently has previously been running the protocol with A as a responder. If the two agents agreed on the data values corresponding to all the variables in the data items, and each such run of A corresponds to a unique run of B.

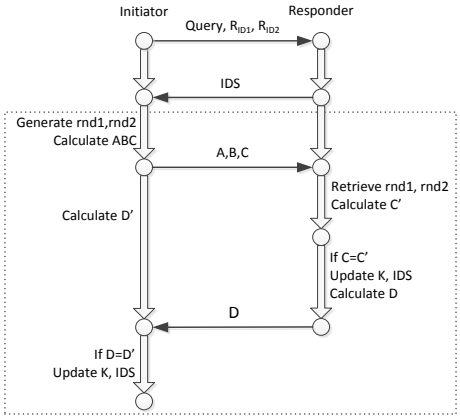


Figure 3.1. Strand space representation of the proposed protocol.

It should be noticed that this definition only guarantees to an initiator agreement with a responder. To complete the proof of the authentication, it is also necessary to prove that the protocol guarantees to a responder agreement with an initiator. We will start with the proof of the latter one. Additionally, since the first two data exchanges $\{R_{ID1}R_{ID2}, IDS\}$ are broadcasted in the form of cleartext and do not contain any secrets, we will not include them in the following analysis.

Proposition 1: Suppose

1) Σ is a S_{OT} strand space, Γ is a bundle in Σ, and s is a responder strand in $s \in Resp[\cdot]$

2) $K_{A1}^{-1}, K_{A2}^{-1}, K_B^{-1}, K_{C1}^{-1}, K_{C2}^{-1}$ and K_D^{-1} are unknown to all the principals. $K \notin Key_P$.

3) $rnd1$ and $rnd2$ originate uniquely in Σ.

If all the variables agree ($C = C'$ and $D = D'$), then Γ contains a unique initiator's strand $t \in Init[\cdot]$.

This proposition is illustrated in Figure 3.2. We will use two lemmas to prove this proposition. Throughout the remainder of this section, we will fix an arbitrary Σ and let Γ, s, $K_{A1}^{-1}, K_{A2}^{-1}, K_B^{-1}, K_{C1}^{-1}, K_{C2}^{-1}$, K_D^{-1}, $rnd1$ and $rnd2$ satisfy the hypotheses of Proposition 1.

Lemma 1: Let n be the node from which $rnd1$ and $rnd2$ uniquely originate in Σ. If $C = C'$, then n belongs to $Init[\cdot]$ and $term(n) = +\{ABC\}$. In addition, to distinguish, we will later designate this particular node n as n_{i1}.

Proof: Let n^+ be the node that proceeds n_{r1} immediately. (n^+ may be a penetrator doing replay attack.) Then $term(n^+) = +\{ABC\}$. From (3) together with the assumption that K_{C1}^{-1} and K_{C2}^{-1} are unknown, we have $rnd1, rnd2$, and $K \subset \{ABC\}$ and thus

$$rnd1, rnd2, K \subset term(n^+) \tag{5}$$

Now if we can show "$K \subset term(n)$" then we are able to conclude that $n \in Init[\cdot]$. This is because 1) $K \notin Key_P$ which implies that $n \notin P$; 2) Although $K \in Key_R$, $rnd1$ and $rnd2$ do not originate from $Resp[\cdot]$ according to (5). Based on the definition of node n, it follows that $n \notin Resp[\cdot]$. Therefore, the problem becomes to prove $K \subset term(n)$.

Now we assume $K \not\subset term(n)$; from (5) we know $K \subset term(n^+)$, then there exists at least one node n' that proceeds n^+ from which K uniquely originates and hence $K \subset term(n')$. Since $K \notin Key_P$, it follows that n' lies either in the responder's or the initiator's strand. However, according to the definition of S_{OT} strand space, the form of K is either $rnd_1 \oplus \{K, R_{ID1}\}_{K_{A1}} \oplus \{K, R_{ID2}\}_{K_{A2}}$ or $rnd_2 \oplus \{K, rnd1\}_{K_B}$ where $rnd1$ and $rnd2$ are fresh. In other words, $rnd1$ and $rnd2$ also originate from n', which contradicts with the fact that $rnd1$ and $rnd2$ originate from n. Therefore, we have $K \subset term(n)$ and hence $n \in Init[\cdot]$.

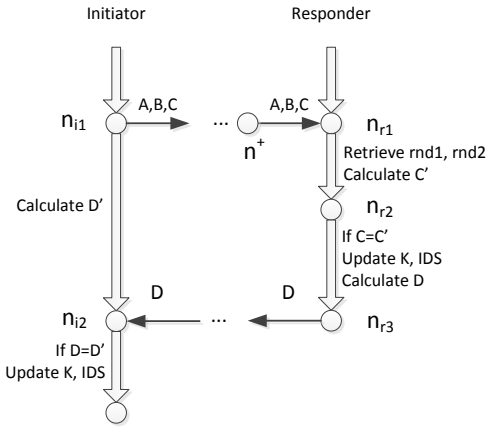


Figure 3.2. Illustration of Lemma 1 and 2.

Moreover, "$rnd1$ and $rnd2$ originate from n" also gives the conclusion that the sign of $term(n)$ is positive (Lemma 2.8 in [44]). Together with $n \in Init[\cdot]$ and the structure of S_{OT}, we can get that $term(n) = +\{ABC\}$.

Lemma 2: Upon receiving D if the node n is able to update K and IDS, then n belongs to $Init[\cdot]$ and n_{i1} (defined in Lemma 1) proceeds node n. In addition, we designate this particular node n as n_{i2}

Proof: If the node n in $Init[\cdot]$ is able to update K and IDS, then $D = D'$. Since $D = \{K^*, IDS^*\}_{K_D}$ where K_D^{-1} is unknown to all principals, it follows that node n must have K^* and IDS^* in the form of cleartext. Then there are two possibilities:

1) $rnd1, rnd2, K \subset term(n)$ in the form of cleartext. Node n computes K^* and IDS^* by itself.
2) Node n receives the cleartext K^* and IDS^* from another node n'. Then $term(n') = +\{K^*, IDS^*\}$. From the form, we can tell that n' does not belong to a regular strand, hence $n' \in P$. Therefore we have $K \in Key_P$ which contradicts with the assumption.

Therefore, only case i) holds and thus $n \in Init[\cdot]$. From $rnd1, rnd2 \subset term(n)$ together with the fact that $rnd1$ and $rnd2$ originates uniquely from node n_{i1}, it follows that n_{i1} proceeds n. Proposition 1 now follows immediately from Lemmas 1 and 2. Note that the uniqueness is also proved by the conclusion of "n_{i1} proceeds node n" because n_{i1} is the node that $rnd1$ and $rnd2$ uniquely originate from. Next we will prove the other side of the authentication: agreement property for the S_{OT} initiator.

Proposition 2: Suppose

1) Σ is a S_{OT} strand space, Γ is a bundle in Σ, and s is a initiator strand in $s \in Init[\cdot]$
2) $K_{A1}^{-1}, K_{A2}^{-1}, K_B^{-1}, K_{C1}^{-1}, K_{C2}^{-1}$ and K_D^{-1} are unknown to all the principals.

3) $rnd1$ and $rnd2$ originate uniquely in Σ.

If the all the variables agree ($C = C'$ and $D = D'$), then Γ contains a unique responder's strand $t \in Resp[\cdot]$.

Similarly, we will use two lemmas to prove Proposition 2.

Lemma 3: Let n be the node in which D originates from in Σ. If $D = D'$ for the node n_{i2} (defined in Lemma 2), then n belongs to $Resp[\cdot]$. In addition, we designate this particular node n as n_{r3}

Proof: The proof of this lemma is almost identical to the proof for Lemma 2. Basically we will show that $\{K^*, IDS^*\} \subset term(n)$ in the form of cleartext. Then it follows that $K \subset term(n)$. Thus we eliminates the case that $n \in P$. Again since the sign of $term(n)$ is positive, together with the form of S_{OT} we are able to conclude that n belongs to $Resp[\cdot]$.

Lemma 4: There exists a unique node n in $Resp[\cdot]$ proceeding n_{r3}, such that $term(n) = -\{ABC\}$, where ABC is given in Lemma 1. In addition, we designate this particular node n as n_{r1}.

Proof: In Lemma 3 we have shown that $\{rnd1, rnd2, K\} \subset term(n_{r3})$. Let n be the $\prec_{minimal}$ member of node n_{r3} in $Resp[\cdot]$. Then by the definition of $\prec_{minimal}$ [44], we have $\{rnd1, rnd2, K\} \subset term(n)$. Since $rnd1$ and $rnd2$ uniquely originate in Σ from node n_{i1} which is proven in Lemma 1, then we have this relationship

$$n_{i1} \xrightarrow{\cdots \{rnd1, rnd2, K\}_{\bullet} \cdots} n \tag{6}$$

Therefore the sign of $term(n)$ is negative. Given that $n \in Resp[\cdot]$, exploring all the forms of responder strands, we have $term(n) = -\{ABC\}$. Since $\{ABC\}$ is computed directly based on $rnd1$ and $rnd2$, it follows that $\{ABC\}$ also originates uniquely from node n_{i1}. Hence $\{ABC\}$ in $term(n)$ is the same term that originated from n_{i1}.

Proposition 2 follows directly from Lemma 3 and 4. And together with Proposition 1, we have completed the proof of authentication.

3.2. SECRECY

Definition 5 (Secrecy [46]): A message m is considered secret if in every bundle of the protocol the penetrator cannot receive m in clear text. In other words, there exists no node n such that term(n) = m.

Proof of secrecy for the proposed protocol is straightforward because of special treatment with the secret key K. From (1) to (4) we can see that, in all messages, every sub-term containing K is in the form of $\{K, \cdot\}_{\hat{K}}$ where $\hat{K}$ belongs to $\{K_{A1}^{-1}, K_{A2}^{-1}, K_B^{-1}, K_D^{-1}\}$ and is unknown to all principals. Therefore, under Assumption 1, we can guarantee the secrecy of K.

4. COMPARISON WITH RELATED PROTOCOLS

The previous section confirmed the correctness of the protocol. Given the proven authentication process and secrecy of data, the protocol is guaranteed to resist the tag impersonation, reader impersonation, replay, and MitM attacks. Such resistance of attacks is an essential requirement in authentication and ownership management protocols.

However, there are several other distinctive requirements for any authentication and ownership management protocol. These requirements include forward and backward privacy, desynchronization and windowing avoidance, and location privacy. To perform a comparison between the proposed ownership management protocol and the previous work, we give an analysis of the protocol in terms of these requirements.

1) Backward privacy: An important aspect to consider with ownership transfer is the privacy of the new owner. The old owner should not be able to update the secret keys in order to have copies of the keys of the new owner. In the proposed protocol, the use of TTP guarantees that only the new owner can update the keys. The access of the old owner is permanently revoked upon ownership transfer.
2) Forward privacy: Similarly, the new owner of the tag should not be able to deduce the keys that were used by the old owner. If such a case arises, then all previous transactions can be decrypted, which violates the privacy of the old owner. In the proposed protocol, the key update operations depend on the PRNG function which is irreversible. This guarantees that the no message exchanges prior to the ownership transfer would be decrypted.

3) Desynchronization avoidance: The desynchronization problem cannot be completely prevented because the adversary can always choose to block the last conformation message and consequently one party updates the keys while the other one does not. Our solution is that the TTP should always keep a copy of the previous secret keys and the corresponding tag IDS in case of confronting desynchronization attacks. In that case, the new owner will not be able to authenticate the tag and then TTP should attempt to resend the key update message until the ownership transfer succeeds.
4) Windowing avoidance: The windowing problem occurs when the new and old owner share possession of the same keys within the same timeslot. Both parties would have access to the tag and problems may arise if, for example, the ownership transfer is interrupted. In such a case, both parties would have access to the tag and can act as its owners. In the proposed protocol, the old owner and the new owner never possess the master key at the same time.
5) Location privacy: Instead of using the unique and life-long static identifier EPC, the proposed protocol uses IDS which is updated after every successful authentication. As a result, the adversary cannot identify the location of the target tag.

A comparison with previous related work is shown in Table. 4.1, where a "Y" means the scheme satisfies the requirement while an "N" indicates the opposite. From the table it can be concluded that among the non-EPC-compliant protocols, Kapoor's [27] has the best performance but it still suffers from the windowing problem and is not suitable for low-cost RFID tags due to the use of hash functions. On the other hand, the existing EPC compliant protocols either fail to provide backward privacy or are vulnerable to replay attack because of using CRC as the encryption method. In contrast, the proposed protocol

not only conforms to the EPC standards, but also satisfies the security requirements. Furthermore, our protocol also supports delegation, which is desirable in many scenarios where temporal ownership sharing is needed.

Table 4.1. Comparison with previous related work [43].

Schemes	[24] Osaka	[27] Kapoor	[34] Song	[34] Seo	[37] Chen	Our scheme
EPC compliant	N	N	N	Y	Y	Y
Support delegation	Y	N	N	N	N	Y
Resist replay attack	Y	Y	N	N	N	Y
Location privacy	Y	Y	N	Y	Y	Y
Backward privacy	N	Y	Y	N	Y	Y
Desynchronization	N	Y	N	Y	Y	Y
Windowing	N	N	N	Y	Y	Y

5. HARDWARE IMPLEMENTATION AND EVALUATION

In this section, the proposed authentication and ownership management protocol is implemented and evaluated in hardware. Since the new EPC Gen2v2 protocol was ratified very recently, there is no reader available in the market supporting the new standard yet. Our solution is to use a Gen2v1 RFID tag and emulate the Gen2v2-only commands ("Authenticate", "KeyUpdate") by using the "BlockWrite" and "Read" commands. Note that "BlockWrite" command allows the reader to send as long as 256 words of data to the tag and therefore is capable of emulating the above Gen2v2-only commands. As these commands take similar amounts of bits, theoretically the differences in terms of processing time and energy consumption are negligible.

5.1. IMPLEMENTATION DETAILS

The mutual authentication and OT is executed through the use of command/response set defined by the EPC Gen2v2 standard as shown in Figure 5.1. The current (old) owner sends "select" and "query" command (and "QueryAdjust", "QueryRep" commands, if necessary) in order to identify the target tag from a large population of tags. As a result, the target tag replies with a new 16-bit random number RN16 and transfers its state from "ready" to "reply". Note that before identifying the target tag, a probabilistic collision management method is adopted as specified in the standards while after identifying the target tag, RN16 works as a kind of session ID indicating a specified tag to avoid collision. Then the reader issues an ACK command containing the same RN16 and the tag replies with its IDS and other information, which can be found in

the EPC Gen2v2 standard specifications. Upon receiving the “Req_RN” with the correct RN16 and access key, the tag backscatters the new RN16 and enters the “open” state.

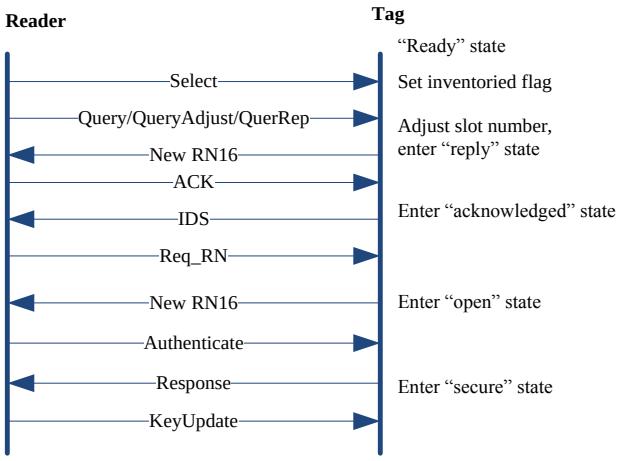


Figure 5.1. Mutual authentication under EPC Gen2v2 standard [43].

Next, we make use of the “Authenticate” and “KeyUpdate” commands, which are newly introduced in EPC Gen2v2, to complete the mutual authentication phase. As specified in [2], the “Authenticate” command should contain fields listed in Table 5.1. In particular, we define the contents of “message” field in the “Authenticate” command as described in Table 5.2. The “command ID” is used to indicate that this command will send the necessary security parameters (RID, A, B…) and start the authentication phase.

Table 5.1. Authenticate command [2][43].

	Command	RFU, SenRep…	Length	Message	RN	CRC
# of bits	8	…	12	variable	16	16
Comments	11010101	Details in EPC Gen2v2 standards[2]				

Table 5.2. “Message” field in “authenticate” command [43].

	Command ID	RID1	RID2	A	B	C
# of bits	8	96	96	96	96	96
Comments	00000001	Details in Figure 2.1				

The value D is contained in the response message of the “Authenticate” command, as described in Table 5.3. A non-zero value in the “status” field indicates that the tag has retrieved the nonces and computed the new key and IDS. Upon receiving a response with the “status” of success, the reader will compute D’ in the same manner of computing D.

Table 5.3. Response message of the “authenticate” command [43].

	Command ID	Status	Length	Message	RN16	CRC
# of bits	8	2	10	96	16	16
Comments	00000010			D		

If D equals to D', then the tag is authenticated. Consequently, the reader issues a "KeyUpdate" command to the tag for confirmation. As a result, the tag commits to the newly computed key and IDS for future uses.

The implementation details of the delegation phase and the ownership transfer phase under EPC Gen2v2 framework are omitted as it is similar to what we have presented in the authentication phase.

A common RFID platform presented in [44] is chosen to implement and analyze the proposed protocol. Operating in the UHF frequency range, this platform is designed based on the Wireless Identification and Sensing Platform (WISP), developed by Intel Research Seattle [44]. Similar to the WISP tags, the program running in the modified WISP tags is also written strictly conforming to the EPC Gen2v1 standard [1]. Therefore, the tag can communicate with most of the off-the-shelf UHF RFID readers.

On the modified WISP tag, shown in Figure 5.2, a "bow tie" antenna and a four-order Dickson charging pump are adopted to convert the RF signal to DC power to support the whole on-board circuitry. The 16-bit microprocessor MSP430F2132 has an ultra-low power consumption (only 600μA at 1.8V and 4MHz). It can execute an instruction in as little as 0.25μs.

Further, the 1Mbit EEPROM 24AA1026 embedded only on the modified WISP tags ensures enough space for storing the data such as secret keys. Therefore, these features including its ability of re-programming, relatively strong computation capacity, and large memory space make it a decent platform to evaluate customized protocols. In fact, the WISP tag was utilized to demonstrate the feasibility or performance of security protocols [49], [49]. Figure 5.3 shows the software structure of our experimental platform.

Figure 5.2. Modified WISP: Class-1 Generation-2 UHF passive RFID tag platform.

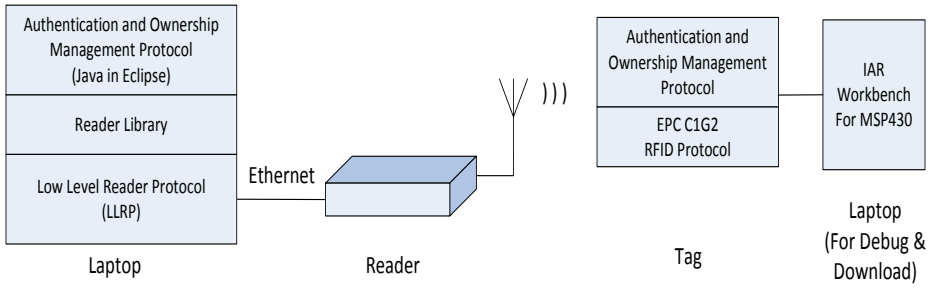


Figure 5.3. Software structure of the evaluation platform.

On the reader side, the protocol is implemented with Java in Eclipse, above the "Reader library" and "LLRP [50]" layers. On the tag side, we implement the proposed protocol in a higher level in order to stay compliant with the EPC standards. The IAR Workbench for MSP430 is used for debugging and downloading the program. The reader used in the experiments is Impinj Speedway Revolution R220, with transmission power set to 30dBm with a receiving sensitivity set to -70dBm.

5.2. OT OPERATION TIME, WITH SUFFICIENT ENERGY

First, it is of interest to measure the execution time for a complete ownership transfer process when there is sufficient energy on the tag. To do this, the tag is placed as close as 0.5m away from the reader antenna to ensure it can harvest enough energy.

Note that no matter how complicated one protocol is, it can be broken into steps that belong to one of the four categories: a) computation on tags, b) computation on readers (here consider TTP as a reader), c) data exchange between tags and readers ($T \leftrightarrow R$), d) data exchange between two different readers ($R \leftrightarrow R$). The results are presented in Table 5.4.

In our case, both the computation on readers and data exchange between two different readers can be negligible. From the results presented in Table 5.4. It can be seen that the total time of on-tag computation plus the data exchange between the reader and the tag is Ttag = 146.14ms, which is quite close to the actual measured total time Ttotal = 167.28ms.

Table 5.4. Measured time and instruction cycles.

Notation	Definition	Value	Cycles
NTR	Number of T↔R rounds	3	-
TTR	Time for each T↔R round	43.16ms	-
Tauth	Time of computation during authentication phase	12.39ms	37170
Ttran	Time of computation on tag during OT phase	4.27ms	12810
Ttag	Ttag = NTR* TTR+ Tauth+ Ttran	146.14ms	-
Ttotal	Actual measured total time	167.28ms	-

In fact, the time spent for the on-tag computation is only 16.66ms (49980 instruction cycles @ 3MHz) for the authentication and ownership transfer phase and 10.83 for the delegation phase (32490 instruction cycles @ 3MHz), which confirms the ultra-lightweight property of the proposed protocol.

5.3. OT OPERATION TIME, WITH INSUFFICIENT ENERGY

Since passive RFID tags are powered by the RF signal emitted by the reader antenna, the energy being harvested decreases when moving away from the antenna. It is also of interest to measure the execution time when there is insufficient energy. For this purpose, the tag is placed at different distances away from the reader antenna and the corresponding number of successful ownership transfer sessions per minute is taken. In contrast, the experiments are repeated using the same tag running the protocol, with all the computations eliminated. In other words, the control group only executes instructions to perform the same number of data exchanges.

From Figure 5.4, it can be seen that when the distance is within 1m, the number of successful ownership transfer session per minute is almost constant because enough energy has been harvested within this short distance. As the distance increases, the number of successful ownership transfer sessions goes down due to failure of data exchange when there is insufficient power.

As a consequence, the reader will either start over a new ownership transfer session or request for a retransmission, which both consume longer time. When the distance is larger than 3m, the proposed protocol with or without computation can only be executed for a very limited number of sessions due to the lack of energy.

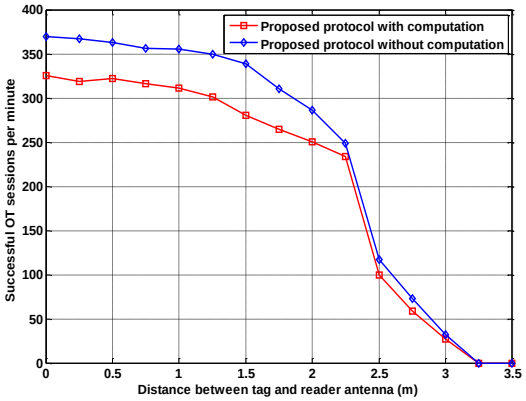


Figure 5.4. Number of successful OT sessions per minute.

However, the most important conclusion is that, if one compares the two curves with each other, the number of sessions executed per minute for the proposed protocol with computation is only slightly less than that the one without computation, which shows that the on-tag computation involved due to the proposed protocol is insignificant.

5.4. OT OF MULTIPLE TAGS, WITH SUFFICIENT ENERGY

In most applications, there may be more than one tag whose ownerships should be transferred. The previous analysis focused on a single tag ownership transfer. However, it is of interest to investigate the performance when multiple tags are exchanged, given that collisions or interference may happen.

In this experiment, we place the tags at a distance of 0.5 m from the reader antenna. The maximum number of tags in this test is 13 in order to ensure that each tag receives sufficient energy from the reader antenna. We initially start with one tag and add more tags until we reach the maximum of 13 tags. For each set of present tags, we measure the

number of successful ownership transfer sessions. For comparative purposes, we also examine the performance with and without the cryptographic computations of the protocol. The results are shown in Figure 5.5. From Figure 5.5, it is evident that as the number of tags increases, the number of successful ownership transfer session decreases. This drop is due to the added extra time caused by the reader when it isolates one specific tag from all the tag population. However, the drop is not that significant in terms of performance. For example, in the case of the protocol without the computations the drop in the successful sessions is about 5.6% and for that with the computation the reduction reaches 2.7%.

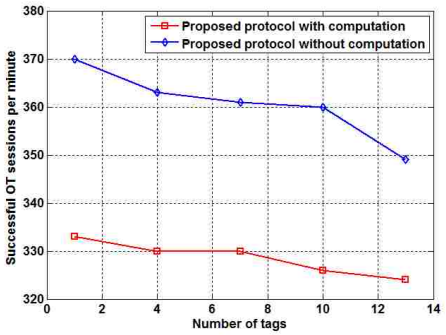


Figure 5.5. Number of successful OT sessions per minute for multiple tags.

The added time when multiple tags are present has a minimal effect on the performance, especially when compared with the average time for one complete ownership transfer process. This is because as specified in [2], once the reader has identified one

certain tag, it will append a unique handle (called “RN16”) at the end of each following message exchange such that the other tags will not respond back, in order to reduce time. This inherent property in the standard results in a favorable performance that meets the requirement to serve multiple tags with the least possible delay.

5.5. LOCATION PRIVACY

As mentioned before, we propose the use of IDS to protect location privacy by updating the IDS after each authentication session. Therefore, it is of interest to examine the degree of difference between the old and updated IDS. To do this, we ran 200 consecutive authentication sessions and recorded each IDS as IDSi, where i = 1, 2, …, 200.

We consider $HD_{avg,cons}$, as the running average of the Hamming distance between the current IDS and all previous values. This is computed as

$$HD_{avg,cons} = (N-1)^{-1}\sum_{i=1}^{N-1} H(IDS_i, IDS_{i+1}) \quad (7)$$

where H(x, y) is the Hamming distance of two 96-bit binary number x and y. This metric measures the difficulty for the attacker to deduce the pattern of IDS generating function from the past message exchanges. The results are plotted in Figure 5.6 against the actual Hamming weight values recorded for each of the 200 authentication sessions. We see from the Figure 5.6 that the running average of the Hamming distance for all pairs of IDS converges to 48, indicating a good degree of randomness. This tells us that any new IDS value will have around 48 bit positions, on average, that differ from the previous IDS value. This is further supported by looking at the actual Hamming weight in Figure 5.6.

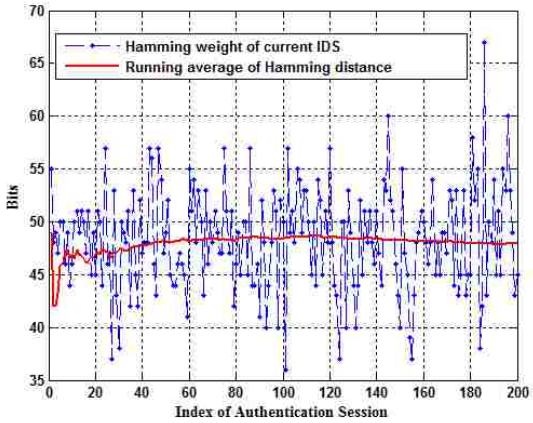


Figure 5.6. Hamming weight of IDS values and average of Hamming distance.

For consecutive pairs, we see a fluctuation in the Hamming weight above or below the overall average for consecutive pairs, which is essential to deny an attacker the chance of tracking the tag. The Hamming weight for the IDS values ranges from 36 to as high as 67. As a result, the attacker cannot determine the presence of the tag by analyzing the values of IDS. Next the reader impersonation aspect is considered.

5.6. READER IMPERSONATION

In this scenario, the attacker impersonates an owner attempting to deceive the tag to believe that the attacker is authentic. Assuming the IDS of the tag has been disclosed, the attacker generates two random numbers (rnd1, rnd2), guesses a secret key, computes the values of A, B, and C, and sends them to the tag. Upon receiving A and B, the tag retrieves rnd1 and rnd2 using the authentic secret key, then computes the value of C'. The tag is compromised if C equals to C'. Note that the attacker does not necessarily have to

possess the exact authentic key to make C'=C. In some circumstances, if the protocol is not well designed, some other different values other than the authentic key could also result in C'=C, this is normally referred to as a collision.

If such a scenario happens, the tag will update its secret keys and IDS although the actual owner has not initiated the session. Thus, the owner and the tag will be desynchronized. Therefore, it is of interest to examine how long it takes the attacker to compromise the tag. Note that it is unrealistic to measure the elapsed time if the length of all data units is 96 bits as it takes too long. To solve this, we truncate the data length to 16 bits, measure the elapsed time, and based on that, estimate the theoretical time for when the data units are 96-bit long. We repeat the attack 50 times and compute the average time for compromise. The results are shown in Figure 5.7, where we see when the length of all data is 16 bits; the average time to compromise the tag is 18 hours, on average.

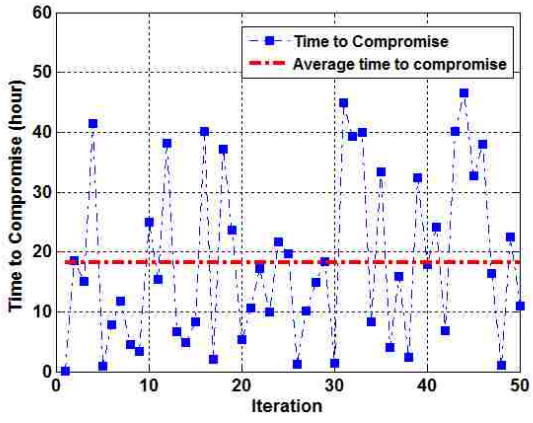


Figure 5.7. Compromise time for 50 iterations of the brute force attack.

As shown before, in an authentication round, the computation takes much less time than the wireless messages exchange. Therefore, if we assume that the time for computing 96-bit long numbers (A, B…) is very close to that for computing 16-bit long numbers, we roughly estimate that the time for the attacker to compromise the tag through brute force when the data units are 96-bit long is $(18/2^{16})\times(2^{96}) \approx 2.1\times10^{25}$ hours.

Therefore, it is safe the say that the proposed protocol is able to resist against the reader impersonation attacks.

6. CONCLUSIONS AND FUTURE WORK

In this paper, a new EPC Gen2v2 compatible protocol by using limited cryptographic functionality was presented for mutual authentication and ownership management. This was done by employing the ultra-lightweight permutation operation and the PRNG function. Such use of a simple operation adds a minimal level of computation and energy consumption while, at the same time, supports the cryptographic goals of the protocol.

The protocol was examined both from a security point of view as well as with a hardware implementation. The analysis indicated that the transactions in the protocol do not expose the secret key information nor does the protocol depend on previously used secret keys, thus guaranteeing that replay or disclosure attacks are not possible. The comparison with previous work shows that the proposed protocol not only conforms to the EPC standards, but also satisfies the security requirements. The hardware implementation supports our initial goal of adding security to the existing EPC Gen2v2 based tags such that the system would be secure both in the case of being used by a single owner or in the more practical cases of having multiple owners during the lifetime of a tagged item.

The next steps in this work include examining the use of various ultra-lightweight or lightweight functions that would possibly fit on the very limited number of gate elements on the tag.

7. REFERENCES

[1] EPC Radio-Frequency Identity Protocols, Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz–960 MHz, Version 1.2.0, EPC Global, 2008.

[2] EPC Radio-Frequency Identity Protocols, Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz–960 MHz, Version 2.0.0, EPC Global, Nov., 2013.

[3] A. Juels and S. Weiss, "Authenticating pervasive devices with human protocols," In Proc. Advances in Cryptology (CRYPTO 2005), Lecture Notes in Computer Science, vol. 3621, pp. 293–308, 2005.

[4] M. Feldhofer and C. Recberger, "A case against currently used hash functions in RFID protocols," in RFID Sec, 2006.

[5] A. Juels, "RFID security and privacy: A research survey," IEEE Journal on Selected Areas in Commun, vol. 24, no. 2, pp. 381-394, Feb. 2006.

[6] H.-Y. Chien, "SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity," IEEE Transactions on Dependable and Secure Computing, vol. 4, no. 4, pp. 337-340, Oct.-Dec. 2007.

[7] M. Morshed, A. Atkins, and Y. Hongnian, "Privacy and security protection of RFID data in e-passport," The 5th International Conference on Software, Knowledge Information, Industrial Management and Applications (SKIMA), Sept. 2011.

[8] M. Wang, Y. Tang, F. Shi, and J. Pan, "An effective RFID authentication protocol," the 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), pp. 141-144, 2012.

[9] Y. S. Lee, T. Y. Kim, and H. J. Lee, "Mutual authentication protocol for enhanced RFID security and anti-counterfeiting," the 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 558-563, March 2012.

[10] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," Workshop on Cryptographic Hardware and Embedded System, M. Joye and J.-J. Quisquater, Eds. New York: Springer-Verlag, 2004, vol. 3156, Lecture Notes in Computer Science, pp. 357–370.

[11] Y. Oren and M. Feldhofer, "A low-resource public-key identification scheme for RFID tags and sensor nodes," the 2nd ACM Conference on Wireless Network Security (WiSec '09), pp. 59-68, 2009.

[12] M. Braun, E. Hess, and B. Meyer, "Using elliptic curves on RFID Tags," International Journal of Computer Science and Network Security, Vol. 8, No. 2, pp. 1-9, 2008.

[13] M. David and N. Prasad, "Providing strong security and high privacy in low-cost RFID networks," Security and Privacy in Mobile Information and Communication Systems (MobiSec 2009), pp. 172–179.

[14] P. Peris-Lopez, J. Hernandez-Castro, A. Tapiador, and A. Ribagorda, "Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol," 9th International Workshop on Information Security Applications, 56-68, 2009.

[15] P. D'Arco and A. De Santis, "On ultralightweight RFID authentication protocols," IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 4, pp. 548-563, July-Aug. 2011.

[16] Y. Tian, G. Chen, and J. Li. "A new ultralightweight RFID authentication protocol with permutation," IEEE Communications Letters, Vol. 16, No. 5, pp. 702-705, May 2012.

[17] H.-Y. Chien and C.-H. Chen, "Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards," Computer Standards & Interfaces, vol. 29, no. 2, pp. 254-259, 2007.

[18] D. Han and D. Kwon, "Vulnerability of an RFID authentication protocol conforming to EPC class 1 generation 2 standards," Computer Standards & Interfaces, vol. 31, pp. 648-652, 2009.

[19] P. Peris-Lopez, J. Hernandez-Castro, A. Tapiador, and A. Ribagorda, "Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard," Computer Standards & Interfaces, vol. 31, pp. 372-380, 2009.

[20] P. Peris-Lopez, J. Hernandez-Castro, A. Tapiador, and J. van der Lubbe, "Cryptanalysis of an EPC class-1 generation-2 standard compliant authentication protocol," Engineering Application of Artificial Intelligence, vol. 24, pp. 1061-1069, 2011.

[21] C.-H. Chen and Y.-Y. Deng, "Conformation of EPC class 1 generation 2 standards RFID system with mutual authentication and privacy protection," Engineering Application of Artificial Intelligence, vol. 22, pp. 1284-1291, 2009.

[22] M. Safkhani, N. Bagheri, and M. Naderi, "Strengthening the security of EPC c-1 g-2 RFID standard," Wireless Personal Communications, Vol. 72, No. 2, pp 1295-1308, 2013.

[23] J. Saito, K. Imamoto, and K. Sakurai, "Reassignment Scheme of an RFID Tag's Key for Owner Transfer," In T. Enokido, L. Yan, B. Xiao, D. Kim, Y. Dai, and L.T. Yang, editors, Embedded and Ubiquitous Computing – EUC 2005 Workshops, LNCS volume 3823, pp. 1303–1312, Springer, Berlin, November 2005.

[24] D. Molnar, A. Soppera, and D. Wagner, "A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags," SAC, vol. 3897, pp. 276-290, 2006.

[25] S. Fouladgar, and H. Afifi, "A Simple Privacy Protecting Scheme Enabling Delegation and Ownership Transfer for RFID Tags," Journal of Communications 2, no. 6, 2007.

[26] K. Osaka, T. Takagi, K. Yamazaki, O. Takahashi, "An efficient and secure RFID security method with ownership transfer," International Conference on Computational Intelligence and Security, vol. 2, pp.1090-1095, 2006.

[27] G. Kapoor and S. Piramuthu, "Single RFID tag ownership transfer protocols," IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, Vol. 42, No. 2, pp. 164-173, March 2012.

[28] H.-B. Chen, W.-B. Lee, Y.-H. Zhao, and Y.-L. Chen, "Enhancement of the RFID security method with ownership transfer," Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication, pp. 251-254, 2009.

[29] S. Koralalage, S. Mohammed Reza, J. Miura, Y. Goto, and J. Cheng, "POP method: an approach to enhance the security and privacy of RFID systems used in product lifecycle with an anonymous ownership transferring mechanism," Proceedings of the 2007 ACM symposium on Applied computing, pp. 270-275, 2007.

[30] C. Lim and T. Kwon, "Strong and robust RFID authentication enabling perfect ownership transfer," Conference on Information and Communications Security – ICICS'06, Lecture Notes in Computer Science, vol. 4307, pp. 1–20, 2006.

[31] A. Fernandez-Mir, R. Rasua, J. Roca, and J. Ferrer, "A Scalable RFID Authentication Protocol Supporting Ownership Transfer and Controlled Delegation. RFID," Security and Privacy, LNCS, Volume 7055, pp.147-162, 2012.

[32] T. Dimitriou, "rfidDOT: RFID delegation and ownership transfer made simple," Proceedings of the 4th international conference on Security and privacy in communication networks. article , no 34, 2008

[33] H. Lei and T. Cao, "RFID protocol enabling ownership transfer to protect against traceability and DoS attacks," The First International Symposium on Data, Privacy, and E-Commerce, 2007. pp. 508-510, 2007.

[34] B. Song. RFID Tag Ownership Transfer. In Workshop on RFID Security RFIDSec'08, Budapest, Hungary, July 2008.

[35] L. Kuseng, Z. Yu, Y. Wei, and Y. Guan, "Lighweight mutual authentication and ownership transfer for RFID systems," inProc. IEEE INFOCOM 2010, pp. 1–5, 2010.

[36] Y. Seo, T. Asano, H. Lee, and K. Kim, "A lightweight protocol enabling ownership transfer and granular data access of RFID tags," Proceedings of the Symposium on Cryptography and Information Security, pp. 1–7, 2007.

[37] R. Doss, Z. Wanlei, and Y. Shui, "Secure RFID tag ownership transfer based on quadratic residues," IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp. 390-401, 2013.

[38] C.-L. Chen and C.-F. Chien, "An ownership transfer scheme using mobile RFIDs," Wireless Personal Communications, 2012.

[39] H. Li, J. Hu, L. He, and L. Pang, "Mutual Authentication and Ownership Transfer Scheme Conforming to EPC-C1G2 Standard," 8th international conference on CIS, Guangzhou, 2012.

[40] X. Fu and Y. Guo, "A Lightweight RFID Mutual Authentication Protocol with Ownership Transfer," Advances in Wireless Sensor Networks Communications in Computer and Information Science Volume 334, pp 68-74, 2013.

[41] C. Chen, Y. Huang, and J. Jiang, "A secure ownership transfer protocol using EPCglobal Gen-2 RFID," Telecommunication System, Volume 53, Issue 4, pp 387-399, 2013.

[42] J. Munilla, G. Fuchun, and S. Willy, "Cryptanalysis of an EPCC1G2 standard compliant ownership transfer scheme," Wireless Personal Communications, pp. 1-14, 2013.

[43] H. Niu, E. Taqieddin, and S. Jagannathan, "A Gen2v2 compliant RFID authentication and ownership management protocol," IEEE 39th Conference on Local Computer Networks (LCN), 2014.

[44] F. J. Thayer, J. C. Herzog, and J. D. Guttman, Strand spaces: Why is a security protocol correct? Proc. 19th IEEE Symposium on Security and Privacy, pages 96–109. IEEE Computer Society, 1998.

[45] G. Lowe, A heirarchy of authentication specifications. 10th Computer Securiy Foundations Workshop Proceedings, pages 31-43. IEEE Computer Society Press, 1997.

[46] Y. Li and J. Pang, "An Inductive Approach to Strand Spaces, Formal Aspects of Computing," vol. 25, issue 4 , pp. 465-501, 2013.

[47] H. Niu and S. Jagannathan, "High memory passive RFID tags with multimodal sensor design and application to asset monitoring in-transit," IEEE International Instrumentation and Measurement Technology Conference, May 2013.

[48] A. P. Sample, D. J. Yeager, P. S. Powledge, A. V. Mamishev and J. R. Smith, "Design of an RFID-based battery-free programmable sensing platform," IEEE Transactions on Instrumentation and Measurement, vol. 57, no. 11, pp. 2608-2615, Nov. 2008.

[49] M.-J. Chae, D. J. Yeager, J. R. Smith, and K. Fu, "Maximalist cryptography and computation on the WISP UHF RFID tag," In Proceedings of the Conference on RFID Security, 2007.

[50] C. Pendl, M. Pelnar, and M. Hutter, "Elliptic curve cryptography on the WISP UHF RFID tag," 7th International Workshop, RFIDSec 2011, Amherst, USA, June 26-28, 2011.

[51] EPCglobal, "Low Level Reader Protocol (LLRP) Version 1.1 Ratified Standard," Oct, 2010.

II. OPTIMAL DEFENSE AND CONTROL OF DYNAMIC SYSTEMS MODELED AS CYBER-PHYSICAL SYSTEMS

Haifeng Niu and S. Jagannathan

With the increasing connectivity among computational cyber-connected elements and the physical entities, a unified representation that captures the interrelationship between the cyber and the physical systems becomes increasingly important. In this paper, we propose a novel representation for developing cyber security schemes for physical systems wherein the cyber system states affect the physical system and vice versa. Subsequently by using this representation, an optimal strategy via Q-learning is derived for the cyber defense in the presence of an attack. Since the cyber system under attack will affect the physical system stability and performance, an optimal controller by using Q-learning is considered for the physical system with uncertain dynamics. As an example, cyber-attacks that increase the network delay and packet losses are considered and the goal of the proposed cyber defense and optimal controller is to thwart the attack and mitigate the performance degradation of the physical system due to increased delays and packet losses. An illustrative example is given where the proposed theory is evaluated on the yaw-channel control of an unmanned aerial vehicle (UAV). Simulation results show that on the cyber side, both the attacker and the defender gains their greatest payoff whereas on the physical system side, the optimal controller is able to maintain the linear system in a stable manner when the cyber state vector meets a certain desired criterion.

1. INTRODUCTION

Cyber-physical systems (CPS) refer to engineered systems constructed as networked interactions of physical and computational cyber components [1]. Examples of CPS can be found in areas as diverse as automobiles, air transportation, civil infrastructure, power grid, embedded medical devices, and consumer appliances. Recently, with the development of information technology (IT) such as IT management and networking growth, the security in CPS has received attention. Moreover, as cyber and physical capabilities are becoming increasingly intertwined, a comprehensive framework that models the cyber system, the physical plant dynamics, and their interrelationship is also increasingly needed.

In general, there are two types of the representations for the security analysis of CPS in the existing literature: one that models the effect on the cyber systems under a certain specific attack [2-6] and the other includes the effect of cyber-attacks on physical systems [7-12]. The former effort explores the behavior of the attacker as well as the defender, formulates the cyber changes under attacks, and presents appropriate strategies that bring the cyber system back to normal. For example, the effort in [2] introduces the Denial of Service (DoS) flooding attacks by a continuous-time Markov chain and utilizes the state space method to compute security measures accurately.

Different from [2], the authors in [3] study the cyber defense by modeling the actions of the attacker and the defender as a stochastic zero-sum game. In [4], the measure of vulnerabilities in cyber-physical systems with application to power systems is defined and a security framework including anomaly detection and mitigation strategies is provided. The authors in [5] evaluate the cyber security by computing the expected

probabilities of the attacker and using the probabilities to build a transition model through game-theoretic approach. In [6], the cyber vulnerability is dynamically evaluated by using hidden Markov model which provides a mechanism for handling sensor data with different trustworthiness. However, this type of representation mainly focuses on the cyber system and neglects the fact that the states of the physical system also affect the cyber defense strategy.

In contrast, others [7-12] concentrate on characterizing the dynamics of the physical system under attacks by extending the classic state-space description in order to include the attacks. For instance, in [7], the system dynamics include an extra term to model the deception attack. In [8], the system state under attack is represented with an additive term where the additive term is used to simulate the false data injection attack. Unlike [8], the authors in [9] characterize the deception attackers by a set of objectives and propose policies to synthesize stealthy deceptions attacks in both linear and nonlinear estimators. In [10], the estimation and control of linear systems when sensors or actuators are corrupted by an attacker is provided, together with a secure local control loop that can improve the resilience of the system. On the other hand, the authors [11] define the control input under attacks as the product of the given input and a coefficient to characterize the effect induced by the DoS attacks. A class of human adversaries, who are called correlated jammers, is considered in [12]. By modeling the coupled decision making process as a two-level receding-horizon dynamic Stackelberg game, the authors propose a control law and analyze the performance and the closed-loop stability under attacks.

However, there are many weaknesses [13] in the above reported works. First, the representation can only describe a single type of attack due to the fact that attacks affect

the system dynamics in a variety of ways. In particular, the author in [13] proposed a unified framework that is able to detect attacks however it still has the two drawbacks mentioned next. Second, it is difficult to implement the representation developed in the literature so far since the system dynamics under attacks are considered known. For instance, due to random delays and packet losses caused by certain cyber-attacks, the physical system dynamics can be uncertain. Last but not the least, these representations fail to take the interactions between the cyber defense policy and the system controller under consideration.

In summary, to the best knowledge of the authors, little effort has been carried out in the literature to develop a representation that precisely characterizes the interplay between the cyber and the physical systems. Such a representation is necessary because inadequate decisions can be made for the cyber defense if the physical states are ignored. Likewise, the physical plant may not be stable if the controller is designed without considering the impact due to the changes in the cyber system.

Therefore, in this paper, we propose a framework for cyber-physical systems to 1) study optimal defense to mitigate attacks and 2) to derive an associated optimal control policy for physical systems. First, we introduce a mathematical representation for the cyber-physical system, in which it was shown that the activities of the cyber system affect the states of the physical system and vice versa. Then based on this representation, we derive the optimal strategies for the defender and the attacker by considering them as two players in a zero-sum game. Since the cyber state influences the behavior of the physical system, next, an optimal controller for the physical system in the presence of uncertainties induced by the cyber system is revisited based on [14]. In addition, a condition on the cyber

state vector is derived under which the physical system is stable. Finally, an illustrative example is given in which we show that on the cyber side, both the attacker and the defender gain their greatest payoff while on the physical side, the optimal controller is able to maintain the plant stable when the state vector of the cyber system meets a certain condition.

Thus, the main contributions of this work include: 1) a novel and comprehensive representation of the cyber-physical system that captures the interrelationship between the cyber and the physical elements; 2) the development of the optimal strategies for the defender and the attacker; 3) the application of the optimal controller [14] for the physical system in the presence of uncertain dynamics induced by the cyber system; and 4) the demonstration of how the proposed theory can be applied to the control of the yaw-channel of an unmanned aerial vehicle (UAV) in the presence of an attack.

The rest of this paper is organized as follows. The proposed representation for the cyber-physical systems is introduced in Section 2. In Section 3, the optimal defense and attack policies are derived and presented, followed by the optimal controller design for the physical system introduced in Section 4. The illustrative example including policy derivation as well as the simulation results are presented in Section 5 and this paper is concluded in Section 6.

2. PROPOSED REPRESENTATION FOR CYBER-PHYSICAL SYSTEMS

In this section, the proposed framework for the cyber-physical systems is introduced. Figure 2.1 depicts the proposed representation for the optimal defense scheme.

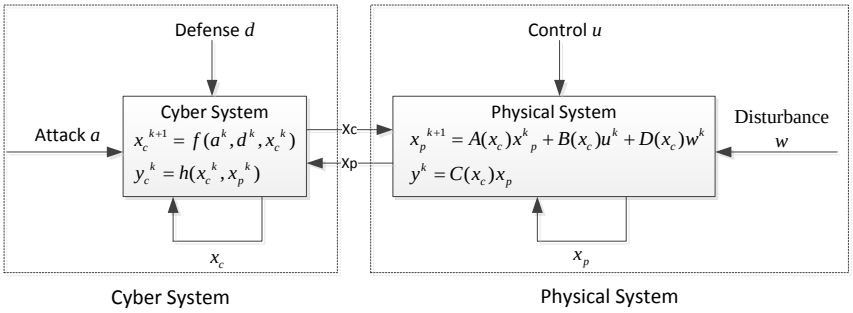


Figure 2.1. Proposed representation of a cyber-physical system.

2.1. CYBER SYSTEM

Consider the cyber system described by a nonlinear discrete-time system given by

$$x_c(k+1) = f\left(a(k), d(k), x_c(k)\right) \tag{1}$$

where $x_c \in \mathbb{R}^{N_c}$ is the state of the cyber system, N_c being the dimension of the state vector of the cyber system, $a \in \mathbb{R}$ is malicious action taken by the attacker, and $d \in \mathbb{R}$ is the defense strategy taken by the cyber system.

The cyber state x_c represents a set of network performance metrics such as latency, throughput, packet loss rate, and so on. Since it was shown in the literature that most attacks on the cyber system will cause an increase in network delay and packet losses [15], in this paper, we mainly consider these two as the cyber state vector in the controller design (Section 4) and in the illustrative example (Section 5). In some cases, x_c also needs to include a few network security metrics such as the number of successive failed authentications or the changes of IP addresses. It is obvious that the cyber state can be affected by the action of both the attacker and the defense strategy and a relationship is described by the function f .

In particular, we propose a more concrete representation of the cyber state as

$$x_c(k+1) = A_c(k)F_c\left(x_c\left(k\right)\right)D_c(k) = \sum_{i=0}^{N_a}\sum_{j=0}^{N_d} a_i d_j f_{ij}\left(x_c(k)\right) \ , \tag{2}$$

where $A_c = \left[a_0, a_1, ..., a_{N_a}\right]$ is a vector consisting of all N_a number of possible attacks, each $a_i \in \{0,1\}$ stands for a type of attack (except for a_0) wherein $a_i = 1$ implies the i th attack has been lunched and $a_i = 0$ otherwise. In particular, we let $a_0 = 1$ if and only if there is no active attack at that moment. Similarly, $D_c = \left[d_0, d_1, ..., d_{N_d}\right]^T$ is a vector describing the status of the defense strategies and $d_0 = 1$ if and only if there is no active defense. Finally, $F = \left[\ f_{00}, f_{01}, ..., f_{0N_d}; ...; f_{N_a 0}, f_{N_a 1}, ..., f_{N_a N_d}\ \right]$ is a matrix of functions and each element $f_{ij} : \mathbb{R}^{N_c \times 1} \to \mathbb{R}^{N_c \times 1}$ describes the effect to the cyber state x_c brought by the ongoing attack/defense pair (a_i, d_j). In other words, at each sampling time instant k, the active attack/defense pair (a_i, d_j) corresponds to a function f_{ij} which characterizes the system dynamics for the following sampling interval.

An assumption is made in that when there are two or more attacks (and defense) simultaneously being lunched, the effect of each attack (and defense) to the cyber system state is independent.

As depicted in Figure 2.1, the cyber system output in the proposed representation is described as

$$y_c(k) = h\left(x_c(k), x_p(k)\right) \ , \tag{3}$$

where $y_c \in \mathbb{R}$ is the output of the cyber system and $x_p \in \mathbb{R}^{N_p}$ is the state of the physical system with N_p being the dimension of the state vector. The output y_c, which is a function of x_c and x_p, is a quantized value indicating the condition of the cyber system. A simple example is presented in Remark 1 whereas more complicated forms can be found in Remark 2.

One can assess the health condition or even the specific attack on the system by exploiting the cyber state x_c as well as the physical system state x_p. For example, if the network is reported with a significant drop in throughput and a considerable mean delay in a short time, then it is possible that the system is experiencing a denial of service (DoS) attack. The importance of introducing the cyber output y_c stems from the fact that the states needs to be organized and interpreted in order to be useful for the administrator to make suitable defense strategies.

It is important to note that the physical system state x_p is also necessary at the cyber system in order to obtain a comprehensive and accurate estimation of the system condition. For example, if an attacker manages to get the administrative privilege without being detected by cracking the password or exploiting the security bugs, then he/she is able to

give malicious instructions that may lead to the failure of the physical system. In this case, only the abnormality in the physical system state (not the cyber state) could be detected. Therefore, by including the physical system state when assessing the condition of the cyber system, the administrator can still trigger the alert mechanism and launch the defense even if no abnormities in the cyber systems have been observed. Therefore, by using both x_c and x_p in y_c, the cyber defense decision becomes more insightful and reliable. The relationship between y_c, x_c, and x_p is characterized by the function h.

Remark 1: A simple example of the cyber output y_c is presented here, in which y_c is defined as

$$y_c = \begin{cases} 1, & if\ x_c \in X_{cd}\ and\ x_d \in X_{dd} \\ 0, & otherwise \end{cases},$$

where X_{cd} and X_{dd} are the set of desired values of the cyber state x_c and physical state x_p respectively. Therefore, in this example, $y_c = 1$ represents a healthy system while $y_c = 0$ represents a compromised one.

Remark 2: The function h may take various forms on the basis of the system security requirement. The selection of h is critical to the system security level, considering that the output of h is used to assess the system health condition and determine the defense strategies that will be launched. The objective of selecting function h is that it should make use of the observed states and precisely predict the ongoing or even potential attacks. A few examples of function h can be given as follows:

1) Threshold form: $y_c = \left(\operatorname{sgn}\left(\begin{bmatrix} x_c - x_{c\_\min} \\ x_p - x_{p\_\min} \end{bmatrix} \right) + \operatorname{sgn}\left(\begin{bmatrix} x_c - x_{c\_\max} \\ x_p - x_{p\_\max} \end{bmatrix} \right) \right) / 2$, where $y_c \in \mathbb{R}^{(N_c+N_p)\times 1}$, $x_{c\_\min}, x_{c\_\max}$ ($x_{p\_\min}, x_{p\_\max}$) are the predefined lower, upper threshold vectors for each

cyber (physical) state respectively and $\mathrm{sgn}(\cdot)$ is the sign function. As a result, the corresponding row of y_c becomes "-1" if a state is smaller than the lower limit, "0" if within the interval, and "1" if higher than the upper limit. This form of function h provides a straightforward assessment of whether the states are in the desired zone or not.

2) Linear form: $y_c(k) = \eta_c x_c(k) + \eta_p x_p(k)$ where $y_c \in \mathbb{R}$; $\eta_c \in \mathbb{R}^{1\times N_c}$ and $\eta_p \in \mathbb{R}^{1\times N_p}$ denote the coefficient vectors for each state. By making use of these weighting factors, this form maps the state vector onto a scalar that provides an approximate description of the system healthy condition.

3) Quadratic form $y_c(k) = x_c^T(k)\Lambda_c x_c(k) + x_p^T(k)\Lambda_p x_p(k)$, where $y_c \in \mathbb{R}$, $\Lambda_c \in \mathbb{R}^{N_c\times N_c}$ and $\Lambda_p \in \mathbb{R}^{N_p\times N_p}$ represent the weighting matrices for each state. Similar to the linear form, this quadratic form also maps the state vector onto a scalar except that it takes the correlation between each state into consideration.

In this paper, the attacks considered will increase the network delay and packet losses which in turn will make the linear time-invariant system as an uncertain stochastic time-varying system. The goal of the cyber defense and optimal controller is to mitigate the increase in random delays and packet losses and performance degradation of the physical system.

2.2. PHYSICAL SYSTEM

As shown in the right block in Figure 2.1, the physical system is described as a linear discrete system in the presence of a disturbance given by

$$\begin{aligned} x(k+1) &= A(x_c)x(k) + B(x_c)u(k) + D(x_c)w(k) \\ y^k(k) &= Cx(k) \end{aligned}, \tag{4}$$

where $x_p \in \mathbb{R}^{n_p}$ is the state of the physical system, $u \in \mathbb{R}^{m_u}$ is the control input, $w \in \mathbb{R}^{m_w}$ is the disturbance input, $y \in \mathbb{R}^{r}$ is the output, and $A \in \mathbb{R}^{n_p \times n_p}$, $B \in \mathbb{R}^{n_p \times m_u}$, $C \in \mathbb{R}^{r \times n_p}$ and $D \in \mathbb{R}^{n_p \times m_w}$ denote the system matrices.

It is important to note that unlike the classical linear discrete system, the system matrices described by (4) are a function of the cyber state x_c. In other words, the state of the cyber system will influence the dynamics of the physical system. For instance, a large network-induced delay or packet loss can degrade the system performance or even results in instability. Therefore, this framework is able to capture the cyber system activities because when a cyber-attack occurs, the physical system matrices $\{A(x_c), B(x_c)...\}$ change.

In conclusion, the cyber state vector, whose update is subject to the attack/defense decisions, changes the physical system dynamics. As a result, the control input needs to be adjusted to drive the physical states back to the desired value. The changes in the cyber and physical states, in turn determine the cyber output and hence the attack/defense decisions. A summary of the interrelationship between the cyber and the physical systems is shown in Figure 2.2.

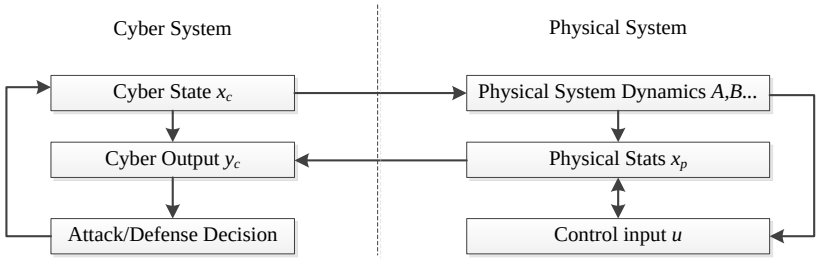


Figure 2.2. Inter-relationship between the cyber and the physical system.

Hence, the objective is to design an optimal policy by using a cost function for the physical system with unknown system dynamics induced by the cyber system. Therefore, by 1) including the physical system state in the assessment of cyber health condition and 2) considering the influence on the physical system dynamics induced by the cyber states when designing the optimal controller, the proposed optimal defense/control scheme offers a coupled" design which is able to capture the influence of the cyber and the physical systems.

3. OPTIMAL ATTACK/DEFENSE POLICY FOR CYBER SYSTEMS

In this section, the optimal attack and defense policies for the cyber system are derived while in the next section, we derive the optimal controller for the physical system with the presence of the delay and packet loss. We also derive the condition for the delay and packet loss under which the physical controller can be stabilized. The optimal controller gain will be computed and applied to the physical system once the delay and packet loss satisfy the condition. Otherwise appropriate defense strategy needs to be launched in order to drive the cyber states (delay and packet loss) to meet the criterion.

In this section, we first model the interactions between the attacker and the defender as a two-player zero-sum Markov game [16]. Then after defining the instant payoff as well as the expected discounted payoff function, we introduce two lemmas to show the existence of the solution of the game and the optimal policy. Next, the Q-function is proposed and it is shown in Theorem 1 that using the Minimax-Q algorithm [17], the Q-function converges to the game value. As a result, the optimal strategies for the defender and the attacker in order to gain their greatest discounted payoff are also derived.

Consider the cyber system with dynamics described by (2) and an output function in quadratic form of the state vectors, i.e. as

$$\begin{aligned} x_c(k+1) &= A_c(k)F_c\left(x_c\left(k\right)\right)D_c(k) = \sum_{i=0}^{N_a}\sum_{j=0}^{N_d} a_i d_j f_{ij}\left(x_c(k)\right) \\ y_c(k) &= x_c^T(k)\Lambda_c x_c(k) \end{aligned}, \tag{5}$$

where the cyber state vector x_c consists of delay and packet loss for illustrative purpose. Then the system can be modeled as a Markov decision process in which the state at the next sampling interval, $x_c(k+1)$, is determined by the state at the current instant, $x_c(k)$,

together with the action pair $(A_c(k), D_c(k))$ launched by the defender and the attacker. The defender and the attacker update their defense strategies based on the condition indicated by y_c, which is a quantified value computed based on the delay and packet loss of the cyber system. In other words, the defender and the attacker launch appropriate actions so as to drive the delay and packet loss into preferred values.

Let Y be the set of all possible values of y_c. Since it is based on the value of y_c that the defender and the attacker decide which action should be taken, the problem becomes deriving the optimal action for each single value of y_c, which is impractical and unnecessary due to the tremendous computation. Therefore, we divide Y into several subsets and study the optimal strategies for each subset rather than for each element. Suppose that Y is divided into N_{yd} disjoint subsets (i.e., $Y = Y_1 \bigcup Y_2 \bigcup ... \bigcup Y_{N_{yd}}$ and $Y_i \bigcap Y_j = \varnothing$ for $i \neq j$) and each subset corresponds to a level of health status. As illustrated in Figure 3.1, Y is divided into eight subsets.

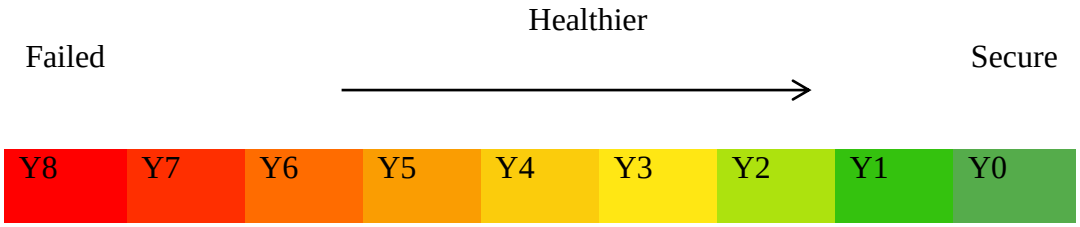


Figure 3.1. Each subset of Y corresponds a level of health condition.

Subset Y_0 is the secure state (with the smallest delay and packet loss) and subset Y_8 is the failed state of the system (with the largest delay and packet loss). The defender decides which action should be taken based on the subset that current y_c is in. For example, if $y_c \in Y_4$, the defender may choose to load the defense more frequently to drive y_c into a more secure subset. As a result, the delay and packet loss are reduced and the physical system becomes more robust and resilient. Obviously, the more subsets Y is divided into, the more accurate the model is. However, more computation is needed as the optimal strategies need to be derived for each subset. Next, the definition of instant reward and discounted payoff are introduced in order to obtain the optimal strategy for each subset Y_i .

Let $r(A_c(k), D_c(k), Y_i(k))$ be the instant payoff (reward or cost) at time instant k in region $Y_i(k)$ for the action pair $(A_c(k), D_c(k))$. Let the instant payoff of the attack and the defender be r_a and r_d respectively and assume the game is zero-sum, we then have the relationship

$$r(A_c(k), D_c(k), Y_i(k)) := r_a(A_c(k), D_c(k), Y_i(k)) = -r_d(A_c(k), D_c(k), Y_i(k)) . \quad (6)$$

Specifically, we let the instant reward be defined as

$$r(A_c(k), D_c(k), Y_i(k)) = x_c^T(k)\Lambda_c x_c(k) + x_p^T(k)\Lambda_p x_p(k) + \xi_d D_c(k) - \xi_a A_c^T(k) , \quad (7)$$

which consists of the cost of the cyber state, physical state, defense, and attack. The defense cost is defined as $\xi_d D_c(i)$ where $\xi_d = \left[\xi_{d,1}, \xi_{d,2}, ..., \xi_{d,N_d}\right]$ and each element $\xi_{d,i} \in \mathbb{R}^+$ is the corresponding cost of launching defense d_i . Likewise $\xi_a = \left[\xi_{a,1}, \xi_{a,2}, ..., \xi_{a,N_a}\right]$ is the vector describing the cost of launching attacks. Next, we will derive the optimal strategy for the attacker and the optimal defense can be obtained in the same manner.

After introducing the definition of the instant payoff, we now consider the expected discounted payoff function over multiple stages. Let $\Xi_A = \{A_c(1), A_c(2), ...A_c(k)...\}$ and $\Xi_D = \{D_c(1), D_c(2), ...D_c(k)...\}$ be the policies for the attack and defense respectively, where $A_c(k)$ and $D_c(k)$ stand for the actions at the time instant k. A policy, which is a sequence of decisions over time, is the mathematical description of a plan of the player for the game [18]. Now define the expected discounted cost function V for each subset Y_i as

$$V(\Xi_A, \Xi_D, Y_i) = \sum_{k=0}^{\infty} \left[\beta^k E\left(r(k) \mid \Xi_A, \Xi_D, y_c \in Y \right)_i \right], \tag{8}$$

where $\beta \in [0,1)$ is the discount factor. As a result, the objective of the attacker becomes finding the appropriate policy Ξ_A in each subset Y_i such that the expected discounted payoff function V is maximized. Correspondingly, the defender aims to find the appropriate defense policy Ξ_D for each Y_i to minimize V. That is to say, we need to solve $\Xi_A = \arg\max_{\Xi'_A} V_a(\Xi'_A)$ and $\Xi_D = \arg\max_{\Xi' D} V_d(\Xi'_D)$. Next, the following two lemmas are introduced before we derive the optimal policies.

Lemma 1. [19] The discounted zero-sum game always possesses a unique solution yielding the optimal game value.

Lemma 2. [20] The policy (Ξ_A^*, Ξ_D^*) is guaranteed to be optimal if $V(\Xi_A^*, \Xi_D^*, Y_i)$ satisfies the following fixed-point Bellman equation given by

$$V(\Xi_A^*, \Xi_D^*, Y_i) = \min_{\Xi_D} \max_{\Xi_A} \left\{ r(A_c, D_c, Y_i) + \beta \sum_{Y_i'} p(Y_i' \mid Y_i, A_c, D_c) V(\Xi_A^*, \Xi_D^*, Y_i') \right\}, \tag{9}$$

where p is the probability of transitioning from current state Y_i to the next state Y_i' after taking action pair (A_c, D_c).

Based on these two lemmas, we use iterative Q-learning method to search for the game value $V(\Xi_A^*, \Xi_D^*, Y_i)$ in (9). Now define the Q-function for each region Y_i as

$$Q(A_c, D_c, Y_i) = r(A_c, D_c, Y_i) + \beta \sum_{Y_i' \in Y} p(Y_i' \mid Y_i, A_c, D_c) V(\Xi_A, \Xi_D, Y_i') . \tag{10}$$

Accordingly, the optimal action dependent value function Q^* of the game is defined as

$$Q^*(A_c, D_c, Y_i) = r(A_c, D_c, Y_i) + \beta \sum_{Y_i' \in Y} p(Y_i' \mid Y_i, A_c, D_c) V(\Xi_A H^*, \Xi_D^*, Y_i') . \tag{11}$$

From (9) to (11), one can conclude that if the action pair sequence (Ξ_A, Ξ_D) is optimal, the optimal Q-function $Q^*(A_c, D_c, Y_i)$ is equal to the game value function $V(\Xi_A^*, \Xi_D^*, Y_i)$. In other words, we have

$$V(\Xi_A^*, \Xi_D^*, Y_i) = \min_{\Xi_D} \max_{\Xi_A} Q^*(A_c, D_c, Y_i) = Q^*(A_c^*, D_c^*, Y_i) . \tag{12}$$

The Minimax-Q algorithm proposed in [17] is adopted to obtain $Q^*(A_c, D_c, Y_i)$ since it provides strong convergence guarantees according to the following theorem.

Theorem 1. Let the Q-function $Q(A_c, D_c, Y_i)$ and the optimal action dependent value function, $Q^*(A_c, D_c, Y_i)$, be defined as in (10) and (11) respectively. Then $Q(A_c, D_c, Y_i)$ converges to the optimal value $Q^*(A_c, D_c, Y_i)$ after an infinite number of iterations with the following tuning law given by

$$Q_{i+1}(A_c, D_c, Y_i) = (1 - \alpha(i)) Q_i(A_c, D_c, Y_i) + \alpha(i)\left(r(A_c, D_c, Y_i) + \beta \Theta_a(Y_i')\right), \tag{13}$$

where $\alpha(i) \in \mathbb{R}^+$ is the learning rate that satisfies $\sum_{i=1}^{\infty} \alpha(i) < \infty$ and $\sum_{i=1}^{\infty} \alpha^2(i) < \infty$, and $\Theta_a(Y_i)$ is called the state value function [17] calculated by

$$\Theta_a(Y_i) = \min_{D_c} \sum_{A_c} Q(A_c, D_c, Y_i) \pi_a(A_c, Y_i), \tag{14}$$

where $\pi_a(A_c, Y_i)$ denotes the probability for the attacker to take action A_c given $y_c \in Y_i$. The proof of Theorem 1 is similar to the theorem in [21].

In addition, since $\pi_a(A_c, Y_i)$ is unknown, linear programming is employed to approximate it at each iteration. An appropriate update law for $\pi_a(A_c, Y_i)$ is given by [21]

$$\pi_a(A_c, Y_i) := \underset{\pi_a(Y_i,\cdot)}{\arg\max} \left\{ \min_{D_c} \left\{ \sum_{A_c} Q(A_c, D_c, Y_i) \pi_a(A_c, Y_i) \right\} \right\} . \tag{15}$$

A flowchart of the proposed method to obtain the optimal defense/attack strategy is shown in Figure 3.2.

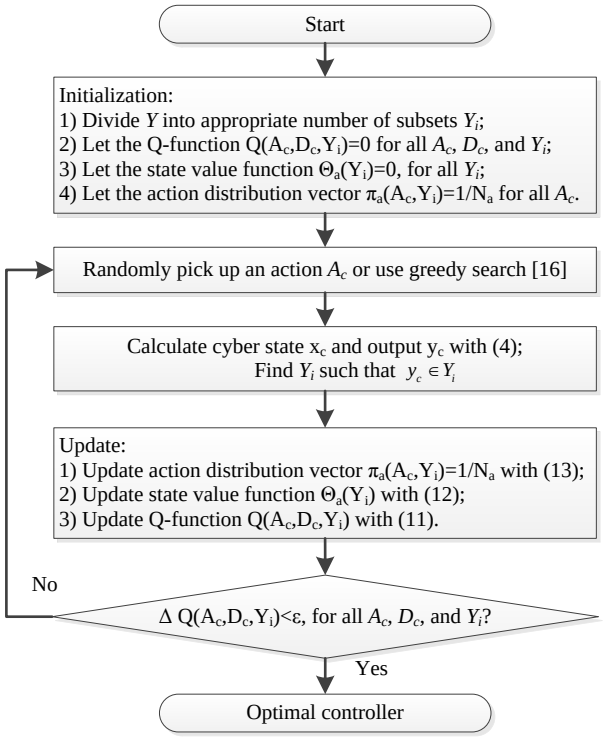


Figure 3.2. Flowchart of the optimal policy for the defender/attacker.

4. OPTIMAL CONTROLLER DESIGN

In this section, we introduce the optimal control scheme for the physical system based on the previous work [14]. First, we model the linear discrete-time system with dynamics that is unknown and altered by the cyber state vector, which includes packet losses and time delays since these are two important metrics for the network that may cause deterioration or potential instability of the system [22]. We then introduce the optimal control gain and show that the system is stable only when the cyber state vector satisfies a certain criterion. The cyber system needs to launch the appropriate defense if its state vector fails to satisfy the criterion. The development of the system dynamics as well as the Q-function update law is taken from the paper [14]. In summary, we show that the cyber state vector affects the optimal controller design and meanwhile the states of physical system also have an impact on designing the defense for the cyber system.

In cyber-physical systems, there are two types of network-induced delays: the sensor-to-controller delay and the controller-to-sensor delay. With the assumption that the former is negligible, the linear continuous system can be described as [14]

$$\dot{x}(t) = Ax(t) + \gamma(t)Bu(t-\tau(t)); \;\; y(t) = Cx(t), \tag{16}$$

where $\gamma(t) = \begin{cases} \mathbf{I}^{n\times n} & \text{if the control input is received at time } t \\ \mathbf{0}^{n\times n} & \text{if the control input lost at time } t \end{cases}$ and τ is the delay which is discrete-value. It is important to note that the data information needed to be discretized before transmitting into the communication network. Moreover, to avoid the infinite-dimensional issue, authors assume that the delays are bounded. Let T_s be the sampling time, the system can be discretized as $x_{k+1} = A_s x_k + \sum_{i=0}^{b} \gamma_{k-i} B_i^k u_{k-i}; \;\; y_k = Cx_k$, (17)

where b is the maximum number of delayed control input during the sampling interval; $x_k = x(kT)$; $A_s = e^{AT}$; $B_0^k = \int_{\tau_0^k}^{T} e^{A(T-s)} dsB \cdot \mathbf{1}(T - \tau_0^k)$; $B_i^k = \int_{\tau_i^k - iT}^{\tau_{i-1}^k - (i-1)T} e^{A(T-s)} dsB \cdot \delta(T + \tau_{i-1}^k - \tau_i^k) \cdot \delta(\tau_i^k - iT)$; $D_i^k = \int_{\tau_i^k - iT}^{\tau_{i-1}^k - (i-1)T} e^{A(T-s)} dsD \cdot \delta(T + \tau_{i-1}^k - \tau_i^k) \cdot \delta(\tau_i^k - iT)$ $\forall i = 1, 2, ..., b$; $\delta(x) = \begin{cases} 1, & x \geq 0 \\ 0, & x < 0 \end{cases}$; and $\gamma_{k-i} = \begin{cases} 1, \text{ if } u_{k-i} \text{ was received during} [kT_s, (k+1)T_s) \\ 0, \quad \text{if } u_{k-i} \text{ was lost during} [kT_s, (k+1)T_s) \end{cases}$. Let the augmented state z_k be defined as: $z_k = [x_k^T \; u_{k-1}^T \cdots u_{k-b}^T]^T$, then the system dynamics become [14]

$$z_{k+1} = A_{zk} z_k + B_{zk} u_k, \; y_k^n = C_z z_k, \tag{18}$$

where the system matrices are a function of the unknown random delays, and packet losses or the cyber state vector which are given by [14]

$$A_{zk} = \begin{bmatrix} A_s & \gamma_{k-1} B_1^k & \cdots & \gamma_{k-i} B_i^k & \cdots & \gamma_{k-b} B_b^k \\ 0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & I_m & \cdots & \cdots & 0 & 0 \\ \vdots & 0 & I_m & \cdots & \cdots & 0 \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & \cdots & I_m & 0 \end{bmatrix}, B_{zk} = \begin{bmatrix} \gamma_k B_0^k \\ I_m \\ 0 \\ \vdots \\ 0 \end{bmatrix}, C_z = \begin{bmatrix} C & & & & & \\ & I_m & & & & \\ & & I_m & & & \\ & & & \ddots & & \\ & & & & I_l \end{bmatrix},$$

and $y_k^n = [y_k^T \; u_{k-1}^T \cdots u_{k-b}^T \; w_{k-1}^T \cdots w_{k-b}^T]^T$ where I_m, I_l are $m \times m$ and $l \times l$ identity matrices. The objective is to minimize the cost function $J_k = \underset{\tau,\gamma}{E}\left(\sum_{m=k}^{\infty} \left(x_m^T S x_m + u_m^T R u_m \right) \right)$ where S and R are symmetric positive semi-definite and symmetric positive definite constant matrices respectively. Applying the augmented state vector, the cost function can be represented as $J_k = \underset{\tau,\gamma}{E}\left(\sum_{m=k}^{\infty} \left(z_m^T S_z z_m + u_m^T R_z u_m \right) \right)$ where $S_z = diag\{S, R/b, ..., R/b\}$ and $R_z = R/b$. The cost function is known to be quadratic and is given as $J_k = \underset{\tau,\gamma}{E}\left(z_k^T P_k z_k \right)$ where $P_k \geq 0$. Define the Q-function as

$$Q(z_k, u_k) = \underset{\tau,\gamma}{E}\left(r(z_k, u_k) + J_{k+1} \right) = \underset{\tau,\gamma}{E}\left(\left[z_k^T, u_k^T \right] H_k \left[z_k^T, u_k^T \right]^T \right) = \left[z_k^T, u_k^T \right] \underset{\tau,\gamma}{E}\left(H_k \right) \left[z_k^T, u_k^T \right]^T, \tag{19}$$

where $r(z_k,u_k)=z_m^T S_z z_m+u_m^T R_z u_m$. Therefore $\underset{\tau,\gamma}{E}(H_k)$ can be expressed in terms of the system matrices as

$$\bar{H}_k=\underset{\tau,\gamma}{E}(H_k)=\begin{bmatrix}\bar{H}_k^{zz} & \bar{H}_k^{zu}\\ \bar{H}_k^{uz} & \bar{H}_k^{uu}\end{bmatrix}=\begin{bmatrix}S_z+\underset{\tau,\gamma}{E}\left(A_{zk}^T P_{k+1}A_{zk}\right) & \underset{\tau,\gamma}{E}\left(A_{zk}^T P_{k+1}B_{zk}\right)\\ \underset{\tau,\gamma}{E}\left(B_{zk}^T P_{k+1}A_{zk}\right) & R_z+\underset{\tau,\gamma}{E}\left(B_{zk}^T P_{k+1}B_{zk}\right)\end{bmatrix}. \tag{20}$$

Consequently, the optimal control gain is represented in terms of $\bar{H}_k$ as $K_k=\left(\bar{H}_k^{uu}\right)^{-1}\bar{H}_k^{uz}$. Moreover, with the linear in the unknown parameters (LIP) assumption, the Q-function can be written as $Q(z_k,u_k)=w_k^T\bar{H}_k w_k=\bar{h}_k^T\bar{w}_k$, where $\bar{h}_k=vec(\bar{H}_k)$, $w_k=[z_k^T,u^T(z_k)]^T$,and $\bar{w}_k=(w_{k1}^2,...,w_{k1}w_{kq},w_{k2}^2,...,w_{kq-1}w_{kq},w_{kq}^2)$ is the Kronecker product quadratic polynomial basis vector. Therefore, the Q-function can be estimated as $\hat{Q}(z_k,u_k)=\hat{\bar{h}}_k^T\bar{w}_k$ in which $\hat{\bar{h}}$ is the estimate value of the target parameter vector $\bar{h}$.

Now define the residual or temporal difference error as $e_{hk+1}=\hat{J}_{k+1}-\hat{J}_k+r(z_k,u_k)$, then we can rewrite the residual dynamics as

$$e_{hk+1}=r(z_k,u_k)+\hat{\bar{h}}_{k+1}^T\Delta W_k \text{ where } \Delta W_k=\bar{w}_{k+1}-\bar{w}_k. \tag{21}$$

Next, we define an auxiliary residual error vector as $\Xi_{hk}=\Gamma_{k-1}+\hat{\bar{h}}_k^T\Omega_{k-1}$ where

$$\Gamma_{k-1}=[r(z_{k-1},u_{k-1}) \quad r(z_{k-2},u_{k-2}) \quad \cdots \quad r(z_{k-1-i},u_{k-1-j})]$$

$$\text{and } \Omega_{k-1}=[\Delta W_{k-1} \quad \Delta W_{k-2} \quad \cdots \quad \Delta W_{k-1-j}].$$

Similarly, the dynamics of the auxiliary vector are derived as: $\Xi_{hk+1}=\Gamma_k+\hat{\bar{h}}_{k+1}^T\Omega_k$. The update law of the target matrix $\bar{H}_k$ is given by

$$\hat{\bar{h}}_{k+1}=\Omega_k\left(\Omega_k^T\Omega_k\right)^{-1}\left(\alpha_h\Xi_{hk}^T-\Gamma_k^T\right). \tag{22}$$

It is shown in [17] that with the update law (22), there exists a positive constant α_h satisfying $0<\alpha_h<1$ such that both the state vectors z_k and the adaptive parameter estimator errors are asymptotically stable in the mean.

Finally, we show the sufficient condition on the cyber state in term of the delay and packet loss that need to satisfy in order to maintain the system to be stochastically stable. Consider the systems with slowly-varying parameters, since the initial stabilizing control and disturbance inputs are given, the linear discrete-time system can be represented as $z_{k+1}=A_{zk}^{*}z_k$ [23]. Applying the linear transformation, the expectation of A_{zk}^{*} can be written as

$$A_{zk}^{*}=\begin{bmatrix} A_s-\gamma_k B_0^k K & \gamma_{k-1}B_1^k & \cdots & \cdots & \gamma_{k-b}B_b^k \\ -K & 0 & \cdots & \cdots & 0 \\ 0 & I_m & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 \\ 0 & 0 & \cdots & I_m & 0 \end{bmatrix} \Rightarrow E\left(A_{zk}^{**}\right)=\begin{bmatrix} E\left(A_s-\gamma_k B_0^k K\right) & E\left(\gamma_{k-b}B_b^k\right) & 0 & \cdots & 0 \\ -K & 0 & 0 & \cdots & 0 \\ 0 & 0 & I_m & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & I_m \end{bmatrix}.$$

According to the definition of stability for stochastic linear time-varying system [24], if eigenvalues of $E\left(A_{zk}^{**}\right)$ are within a unit radius n-dimensional sphere (or disc) for all instants, then the system is stable. Since the eigenvalues of the right bottom block of $E\left(A_{zk}^{**}\right)$ are ones, the left upper block has to satisfy the condition: $\lambda_i[\underset{\tau,\gamma}{E}(A_s-\gamma_k B_0^k K)]<1$ for any i and k and $\lambda(M)$ denotes the eigenvalue of the matrix M. Since K and L are the initial fixed stabilizing control and disturbance input gains for the linear discrete-time system, we have

$$\lambda_i(A_s-B_sK)=\lambda_i^s<1 \text{ with } B_s=\int_0^T e^{A(T-s)}dsB. \tag{23}$$

Then $\underset{\tau,\gamma}{E}(A_s-\gamma_k B_0^k K)$ can be represented as

$$\underset{\tau,\gamma}{E}(A_s-\gamma_k B_0^k K)=A_s-\underset{\gamma}{E}(\gamma_k)\underset{\tau}{E}(B_0^k)K=\left[I-\min\{\Psi_1,\Psi_2\}\right]A_s+\min\{\Psi_1,\Psi_2\}A_s-\Psi_1 B_sK \tag{24}$$

where $\Psi_1=\underset{\gamma}{E}(\gamma_k)\underset{\tau}{E}(\int_{\tau_0^k}^{T}e^{A(T-s)}ds)/\int_0^T e^{A(T-s)}ds$ and $\Psi_2=\underset{\gamma}{E}(\gamma_k)\underset{\tau}{E}(\int_{\tau_0^k}^{T}e^{A(T-s)}ds)/\int_{\tau_0^k}^{T}e^{A(T-s)}ds$.

Combining (23) with (24), we have

$$\lambda_i[\underset{\tau,\gamma}{E}(A_s - \gamma_k B_0^k K)] < \left(1 - \min\{\Psi_1, \Psi_2\}\right) \times \lambda_i(A_s) + \min\{\Psi_1, \Psi_2\}\lambda_i^s .$$

Therefore, in order to maintain stability, the expected values of the delays and packet losses should satisfy

$$\min\{\Psi_1, \Psi_2\} > 1 - \left[1 - \min\{\Psi_1, \Psi_2\}\lambda_i^s\right] / \lambda_i(A_s), \tag{25}$$

where Ψ_1 and Ψ_2 are functions of the delay and packet losses defined by (24). When this inequality is not satisfied, the cyber system needs to launch an appropriate defense to reduce the delay and packet losses in order to prevent instability; otherwise the physical system needs to be halted as it becomes unstable.

5. AN ILLUSTRATIVE EXAMPLE

In this illustrative example, the proposed framework is verified on a small-scale UAV helicopter with remote controller. The objective of the controller design is to stabilize the yaw rotation rate with the presence of two types of cyber-attacks. The attacker aims to maximize the payoff, which are given in terms of the network delay and packet losses in this case, such that the yaw channel becomes unstable. The defender, on the other hand, aims to limit the delay and packet losses under a certain threshold. We will show that on the cyber side, both the attacker and the defender gain their greatest payoff while on the physical system side, the optimal controller is able to maintain the yaw rate stable when the cyber state vector expressed as delay and packet loss meets the derived condition.

5.1. PHYSICAL SYSTEM SETUP

In this illustrative example, we consider the control of the yaw rotation of a small-scale unmanned aerial vehicle (UAV) helicopter. A yaw rotation, as illustrated in Figure 5.1, is a movement around the yaw axis of a rigid body that changes the direction it is pointing [26]. The yaw rotation control is one of the most challenging tasks in controlling small-scale UAVs because even a small control input or disturbance can cause the vibration of the light-weight body [26]. Since it is verified in [27] and [28] that the yaw-channel dynamics for small-scale helicopters can be physically decoupled from other channels, it is reasonable to assume that the yaw-channel dynamic is a single-input-single-out (SISO) system. Furthermore, after applying the prediction-error method [29], an accurate fourth-order model is proposed in [26] as

$$\dot{x} = Ax + Bu;\ \ y = Cx\ ,$$

where $x = [x_1, x_2, x_3, x_4]^T$ consists of the first to the fourth derivatives of the yaw rotation rate; y is the yaw rotation rate that can be measured by a gyro; and

$$A = \begin{bmatrix} -2.66 & 21.94 & 3.83 & 6.05 \\ -31.03 & -3.52 & 17.10 & -3.09 \\ 6.11 & -6.96 & -9.76 & -96.38 \\ 17.17 & 25.73 & 37.18 & -33.08 \end{bmatrix}, B = \begin{bmatrix} 0.63 \\ 6.22 \\ -29.20 \\ -14.64 \end{bmatrix}, C = [15.32 \quad -10.32 \quad 0.73 \quad -4.73].$$

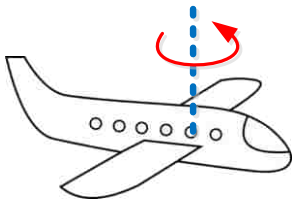


Figure 5.1. Illustration of a yaw rotation.

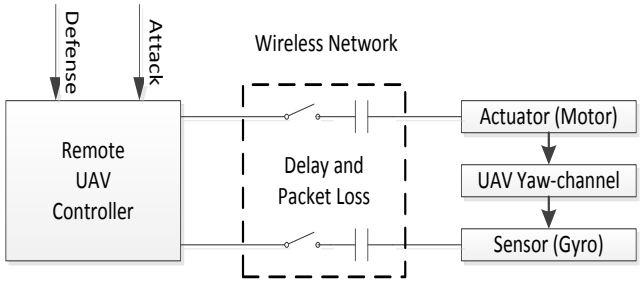


Figure 5.2. Diagram of the UAV with remote controller.

The other parameters of the physical system are introduced as follows. The total simulation time is 200 steps with the sampling time of 100ms and the positive constant α_h equals to 10^{-6}. In the first 50 steps, zero-mean exploration noises with variance of 0.006 and 0.003 are added for the odd and even steps respectively, in order to meet the persistency of excitation (PE) condition. The objective of the controller is to stabilize the yaw rotation rate y by driving the state vector x to zero.

5.2. CYBER SYSTEM SETUP

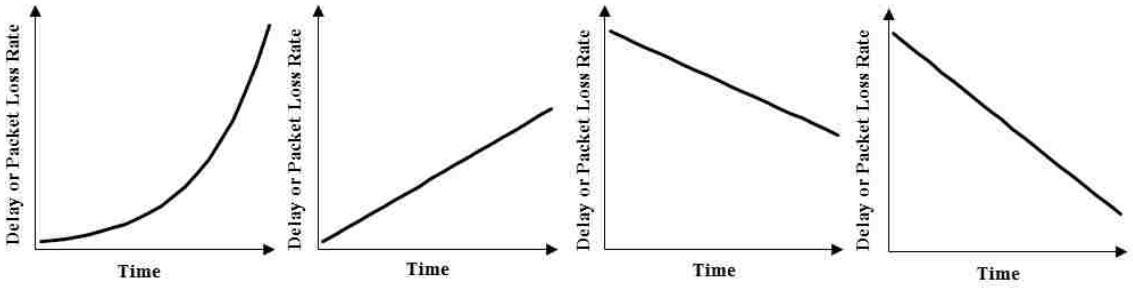
As illustrated in Figure 5.2, we suppose that the UAV is controlled by a base station through a wireless network that suffers from cyber-attacks. As stated earlier, we choose packet losses κ and time delays τ as the cyber state vector in order to evaluate the effect on the network induced by the attack/defense activities, i.e., $x_c = [\kappa, \tau]^T$. Furthermore, smurf attack and slow read attack [30-32] are considered.

Smurf attack is an example of amplification distributed denial of service (DDoS) attack that exploits the unprotected networks to generate significant traffic load on the victim network [30-31].

Slow read attack, on the other hand, tries to exhaust the server's connection pool by sends legitimate application layer request but reads the response slowly [32]. Based on these characteristics, we model the delay and packet loss rate to increase exponentially under the smurf attack and linearly under the slow read attack, which are illustrated in Figure 5.3 (a) and Figure 5.4 (b).

Furthermore, the corresponding strategies that are capable of defending smurf attack and slow read attack are denoted as d_1 and d_2, respectively. We assume that when the appropriate defense strategy is loaded, the packet loss rate and the time delay decrease in a linear manner, which are illustrated in Figure 5.3 (c) and Figure 5.3 (d). In addition, the delay and packet loss rate are modeled to decrease slowly and linearly once the attack is stopped regardless of the action of the defender. For simplicity, we mainly focus on the case where only one attack and one defense are active at a sampling instant. However, it is also briefly shown that the proposed representation can be easily expanded to apply multiple attacks and defenses.

The cyber output is defined as $y_c = x_c^T(k)\Lambda_c x_c(k) + \rho \cdot \delta\left(\left\|x_p\right\| - x_{pt}\right)$, where $\Lambda_c = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$; x_{pt} is the threshold of the physical states; $\delta(\cdot)$ is defined in Section 4. According to this definition, when the physical states are within the threshold, the cyber output is a quadratic function of the cyber state vector only.



(a) (b) (c) (d)

Figure 5.3. Models of delay/packet loss rate under (a) smurf attack, no defense; (b) slow read attack, no defense; (c) smurf attack with the corresponding defense; (d) slow read attack with the corresponding defense.

Next, as presented in the flowchart in Figure 3.2, we divide the cyber output Y into four subsets, i.e., $Y = Y_0 \cup Y_1 \cup Y_2 \cup Y_3$ where Y_0, Y_1, Y_2, Y_3 correspond to the "healthy", "sensitive", "dangerous", and "failed" condition respectively. Moreover, we define the instant reward in the form of (7) with $\xi_d = \left[0, \xi_{d,1}, \xi_{d,2}\right]$ and $\xi_a = \left[0, \xi_{a,1}, \xi_{a,2}\right]$. In other words,

the costs for "not launching any defenses", "launching defense d_1", and "launching defense d_2" are 0, $\xi_{d,1}$, and $\xi_{d,2}$, respectively.

Table 5.1. Summary of system information used in the illustrative example.

Attacks	$A_c = [a_0, a_1, a_2]$, where a_0 demotes "no attacks; a_1 demotes smurf attack; and a_2 denotes slow read attack.
Defenses	$D_c = [d_0, d_1, d_2]^T$, where d_0 demotes "no defenses; d_1 demotes the defense against smurf attack; and d_2 denotes the defense against slow read attack.
Cyber states	$x_c = [\kappa, \tau]^T$, where κ is the packet loss rate and τ is the delay.
System Dynamics	$x_c(k+1) = a_0 d_0 (x_c(k) - \Delta_0) + a_0 d_1 (x_c(k) - \Delta_0) + a_0 d_2 (x_c(k) - \Delta_0) + a_1 d_0 (\xi \cdot x_c(k)) + a_1 d_1 (x_c(k) - \Delta_1) + a_1 d_2 (\xi \cdot x_c(k)) + a_2 d_0 (x_c(k) + \Delta_2) + a_2 d_1 (x_c(k) + \Delta_2) + a_2 d_2 (x_c(k) - \Delta_3)$ where $\Delta_0, \Delta_1, \Delta_2, \Delta_3 \in \mathbb{R}_+^{2\times 1}$ characterize the packet loss rate/delay linearly decrease or increase rate; $\xi > 1$ characterizes the exponentially increasing rate.
Cyber output	$y_c = x_c^T(k) \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} x_c(k) + \rho \cdot \delta(\|x_p\| - x_{pt})$, where $\lambda_1, \lambda_2, \rho, y_c \in \mathbb{R}^+$.
Subsets of cyber output	$Y = Y_0 \cup Y_1 \cup Y_2 \cup Y_3$.
Payoff	$r(A_c(k), D_c(k), Y_i(k)) = x_c^T(k) \Lambda_c x_c(k) + \xi_d D_c(k) - \xi_a A_c^T(k)$, where $\xi_d = [0, \xi_{d,1}, \xi_{d,2}]$ and $\xi_a = [0, \xi_{a,1}, \xi_{a,2}]$.

It is important to note that we make Y_0 be the region with "healthy" condition by setting the cost for launching the defense close to the upper values of Y_1. As a result, if the

cyber output falls into subset Y_0, the defender tends not to launch the defense as it costs more than the payoff brought by the state. Subset Y_1, on the other hand, is modeled as the "sensitive" region where the defender is more likely to launch the defense to avoid the output going into subset Y_2, which is the "dangerous" state in this model. Likewise, if the output falls into region Y_2, there is a very high chance that the defenses needs to be launched to avoid the system going into Y_3, which is the "failed" region.

The system information for this particular example is summarized as in Table 5.1. The simulation is performed with the algorithm described in Figure 3.2 and numerical values shown in Table 5.2.

Table 5.2. Numerical values used in the simulation.

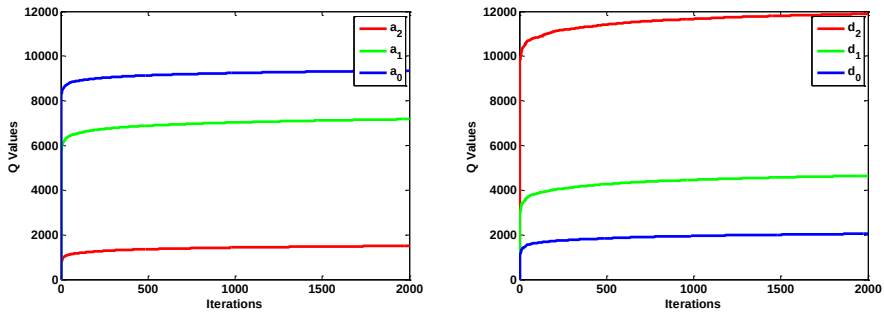
$\alpha(k)=1/k$; $\beta=0.5$; $N_a=N_d=3$; $\xi=1.2$; $\lambda_1=\lambda_2=1$;
$\Delta_0=[1;1.1]$, $\Delta_1=[50;48]$, $\Delta_2=[3;2.9]$; $\xi_d=[0,5000,4500]$; $\xi_a=[0,1500,1000]$;
$Y_0=[0,5000)$, $Y_1=[5000,7200)$, $Y_2=[7200,12800)$, $Y_3=[12800,\infty)$.

5.3. SIMULATION RESULTS

In the simulation, the optimal defense/attack policies for the cyber system and the optimal controller are derived in the presence of delay and packet losses. Since the delay and packet losses are generated from the cyber system, they are determined directly by the policy launched by the defender. After deriving the optimal defense/attack policies, two

scenarios are considered in the simulation. In the first scenario, we let the defender launch the cyber defense policy based on the probability distribution given by the derived optimal policy. By contrast, in the second scenario, the defender selects the defense actions at random.

5.3.1. Results of Deriving the Optimal Attack/Defense Policies. First, we shall show the simulation results of deriving the optimal attack/defense. After about 2000 iterations, the Q-values for all action pairs converge to fixed values. To avoid redundancy, we only show the Q-values for the attacker and the defender in region Y_1 in Figure 5.4 (a) and Figure 5.4 (b), respectively. From Figure 5.4 it can be concluded that the expected discounted payoff for the attacker in region Y_1 is higher if he chooses action a_0 rather than a_1 and a_2. Likewise, the expected discounted payoff values suggest the defender in region Y_i to load action d_2 more frequently than d_0 and d_1. Furthermore, the percentages of the Q-values for each action in the regions are computed and listed in Table 5.3.



(a) (b)

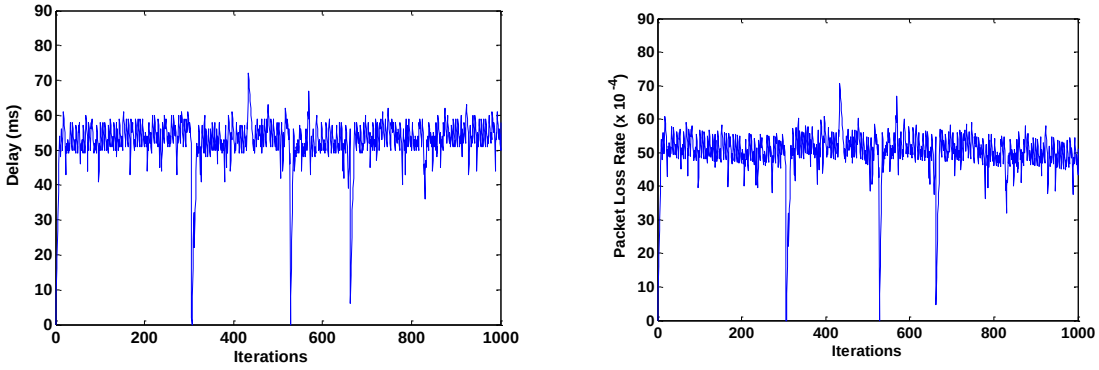
Figure 5.4. Q-values in region for (a) the attacker; (b) the defender.

It can be concluded from Table 5.3 that when $y_c \in Y_0$, the attacker shall take action a_2 more often as it increases the delay and packet losses in a faster way. The defender, on the other hand, shall take no actions, which corresponds to our previous analysis that Y_0 is the region with "acceptable" health condition. With the increase in y_c, the attacker shall slow down the speed to avoid being detected by the defender, as one can conclude from the Q-value distributions in region Y_1 in the table. Correspondingly, the defender starts loading the defense more often in this sensitive region. If the attacker manages to drive y_c into region Y_2 or even Y_3, he shall stop attacking and let the system recover and go back to region Y_1 where he obtains the largest expected payoff. It is important to note that we deliberately design the system as a secure one by letting the recovery speed of the cyber states when appropriate defense is loaded much faster than the degrading speed when the system is under attacks. As a result, the attacker gains the greatest payoff only when y_c is large enough yet not to the degree of being detected by the defender.

Table 5.3. Percentages for each action in the region.

	Attacker			Defender		
	a_0 No attacks	a_1 Smurf Attack	a_2 Slow read attack	d_0 No defense	d_1 Defending smurf attack	d_2 Defending slow read attack
Y_0	0.02	0.58	0.34	0.71	0.09	0.20
Y_1	0.53	0.08	0.39	0.11	0.25	0.64
Y_2	0.69	0.13	0.18	0.04	0.37	0.59
Y_3	0.71	0.13	0.16	0.03	0.40	0.57

The proposed model and analysis is verified through the following simulation. We start the system with the cyber state initialized to zero and stop after 1000 iterations. During iteration, the attacker and defender will 1) determine which region y_c is in and take actions according to the probabilities given by Table 5.3; 2) update the states; and 3) calculate the accumulated payoff. The evolution of the states is shown in Figure 5.5.



(a) (b)

Figure 5.5. Evolution of the states (a) delay; (b) packet loss rate.

From Figure 5.5 it can be concluded that after a rapid increase at the beginning, the delay and the packet loss rate remains relatively stable so that the attacker gains the largest expected payoff in terms of the delay and packet losses. This is achieved by loading much more a_0 (no attacks) than a_1 (smurf attack) and a_2 (slow read attack), as suggested by the probabilities in Table 5.3. Due to the stochastic property of this game, we observe that

occasionally, the attacker loads the "inappropriate" attack (a_1) and detected by the defender, resulting in a significant drop in the states. Figure 5.6 shows the evolution of the output, where one can conclude that as previously analyzed, the output stays in the "acceptable" region at most times, goes to the "dangerous" region occasionally, and never reaches the "failed" region. The averaged payoff for the attacker is shown in Figure 5.7.

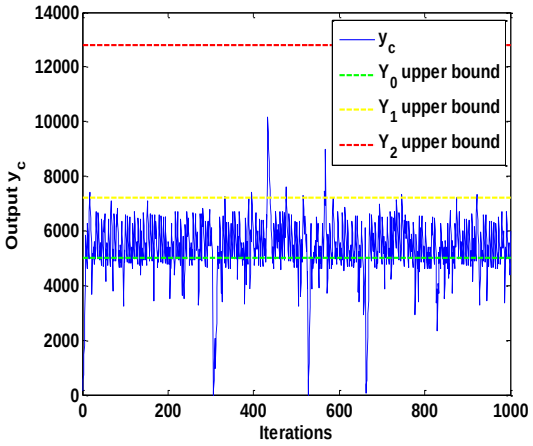


Figure 5.6. Evolution of the output.

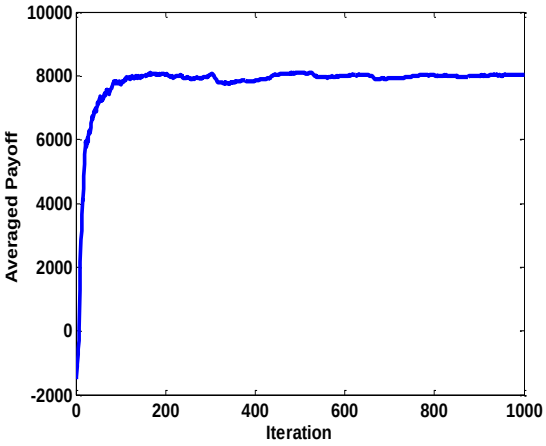


Figure 5.7. Evolution of average payoff.

From Figure 5.7 we can see that after about 100 iterations, the averaged payoff tends to be stable at around 8000, which is the greatest averaged payoff for the attacker. This example shows that by applying the optimal policies the attacker is able to obtain the greatest payoff meanwhile the defender is able to keep the health condition under the "dangerous" level.

In addition, the simulation is repeated for the case where the two attacks/defenses can be loaded simultaneously. As a result, a table similar to Table 5.3 is obtained except that two extra columns are added, which are the probability distributions of simultaneously loading two attacks $(a_1 + a_2)$ and two defenses $(d_1 + d_2)$. To verify the results, we use the method mentioned earlier, in which we observe the output y_c by letting the attacker and defender select their action based on the derived probability distributions. The results are shown in Figure 5.8.

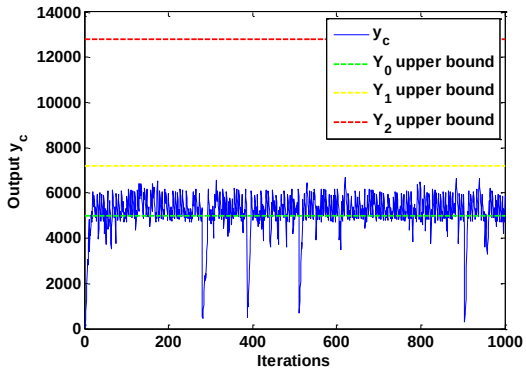


Figure 5.8. Evolution of the output.

From Figure 5.8 one can conclude that the output stays in the "acceptable" region at most times and never goes to the "dangerous" or the "failed" region. This results agree with our previously analysis and verify that the proposed representation can be used in the case where multiple attacks can be loaded simultaneously.

5.3.2. Scenario I: Defender Chooses the Optimal Policy. In this scenario, we let the defender launch the defense policy based on the probability distribution given by the derived optimal policy. As a result, the delay and packet losses have been limited to relatively low values so that the system always stays out of the failed region, which is as verified in Figure 5.5 (a). Consequently, equation (25) is satisfied in this scenario. The simulation results of the regulation errors for the physical system are shown in Figure 5.9, where the state regulation errors converge to zero thus the closed-loop system is stable.

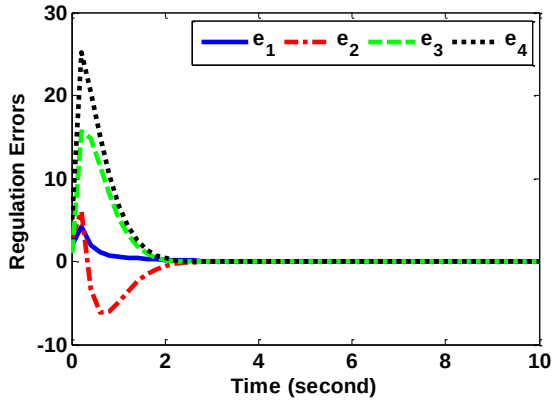


Figure 5.9. Regulation errors in Case I where the cyber defense is optimal.

Therefore, we show that on the cyber side, both the attacker and the defender gains their greatest payoff while on the physical side, the optimal controller is able to maintain the plant stable when the cyber state vector meets the derived criterion.

5.3.3. Scenario II: Defender Chooses a Random Policy. In the second scenario, the cyber defense is selected at random rather than based on the optimal probability distribution given in Table 5.3 As a result, the attacker manages to comprise the system in some cases and the cyber states go far beyond the limit, as verified in Figure 5.10 in which the time delay is plotted.

Consequently, equation (25) cannot be satisfied and thus the system becomes unstable. The regulation errors in this scenario are plotted in Figure 5.11, where it can be seen that the errors do not converge. In summary, the simulation results verify that that the decisions made on the cyber system have an effect on the convergence of the physical system. The system is stable when applying the optimal control in the physical plant and optimal defense policy in the cyber system. If the states go abnormal such that (25) is not satisfied, appropriate actions needs to be launched on the cyber system to bring them back to normal or the physical plant has to be shut down to avoid further damages.

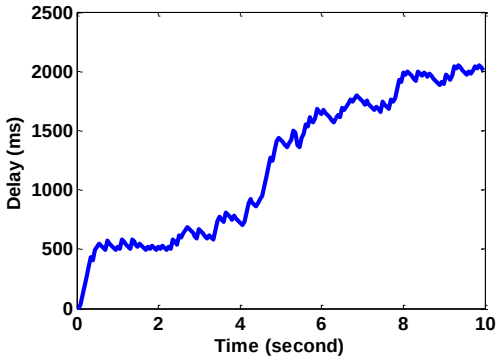


Figure 5.10. Delay in Case II where the cyber defense is randomly selected.

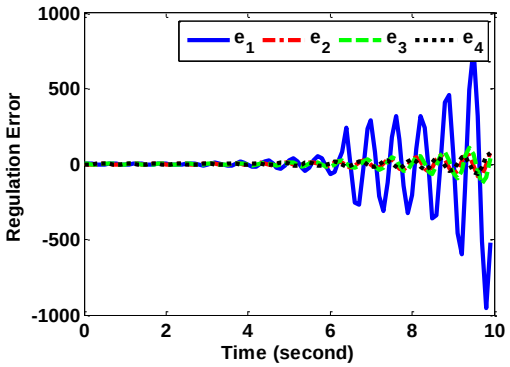


Figure 5.11. System becomes unstable in Case II.

6. CONCLUSIONS AND FUTURE WORK

With the increasing meshing among the cyber-connected elements with the physical entities, the representation for such cyber-physical system becomes more complicated. In this paper, we have proposed a representation that captures the interrelationship between the cyber and physical systems such that the states in the physical system affect the decision made on the cyber systems and vice versa. Based on this representation, the optimal defense and attacks are given to gain the greatest payoff. An optimal controller from the literature is revisited to maintain the stability of the physical system in the presence of the uncertainties induced by the cyber state vector. Since the proposed representation is in a general form, it can be used in a variety of applications including autonomous systems. In particular, the cyber defender is able to make thorough decisions by selecting appropriate cyber state vector and output and customizing the payoff function that is of interest. Meanwhile, there are some recent works focusing on modelling and controlling for multi-agent networks or cyber-physical systems [33-35]. For example, the work in [33] characterizes a binary notion of security and characterizes security levels in terms of the graph matrix and its spectrum, which is complementary to control-theoretic modeling of attacks in cyber-networks and networked control systems. Based on these works, as future work, we can consider studying the impact of different attacks on the network performance to generate a more accurate model for the cyber system dynamics.

7. REFERENCES

[1] Y. Zhou and J. S. Baras, "CPS modeling integration hub and design space exploration with application to microrobotics," Lecture Notes in Control and Information Science, vol. 449, pp. 23-42, 2013.

[2] H. Baumman and W. Sandmann, "Markovian modeling and security measure analysis for networks under flooding DoS attacks," 20th Euromicro International Conferences on the Parallel, Distributed and Network-based Processing, 2012.

[3] Q. Zhu and T. Basar, "Robust and resilient control design for cyber-physical systems with an application to power systems," 50th IEEE Conference on Decision and Control and European Control Conference, 2011.

[4] C.W. Ten, G. Manimaran, and C.C. Liu, "Cybersecurity for critical infrastructures: attack and defense modeling," IEEE Transactions on Systems, Management, and Cybernetics," vol. 40, no. 4, pp. 853-865, July, 2010.

[5] K. Sallhammar, B.E. Helvik, and S.J. Knapskog, "Towards a stochastic model for integrated security and dependability evaluation," IEEE Conference on Availability, reliability and Security, 2006.

[6] A. Aenes, K. Salhammar, K. Haslum, T. Brekne, M. Moe, and S. J. Knapskog, "Real-time risk assessment with network sensors and intrusion detection systems," International Conference on Computational Intellengence and Security, 2005.

[7] C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," American Control Conference (ACC), 2013.

[8] L. Liu, M., Esmalifalak, Q. Ding, V. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," IEEE Transaction on Smart Grid, vol. 5, no. 2, 2014.

[9] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. Sastry, "Cyber security analysis of state estimators in electric power systems," IEEE Conference on Decision Control, December 2010.

[10] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," IEEE Transactions on Automatic Control, vol. 59, no. 6, pp. 1454-1467, 2014.

[11] S. Amin, A. Cárdenas, and S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," Hybrid System Computer Control, vol. 5469, pp. 31–45, April 2009.

[12] M. Zhu and S. Mart ńez, "Stackelberg game analysis of correlated attacks in cyber-physical systems," American Control Conference, July, 2011.

[13] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," IEEE Transaction on Automatic Control, vol. 58, no. 11, 2013.

[14] H. Xu, S. Jagannathan, and F.L. Lewis, "Stochastic optimal control of unknown linear networked control system in the presence of random delays and packet losses," Automatica, vol. 48, pp. 1017-1030, 2012.

[15] H.L. Nguyen and U.T. Nguyen, "Study of different types of attacks on multicast in mobile ad hoc networks," IEEE International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL), 2006.

[16] M. Lagoudakis, R. Parr, "Value function approximation in zero-sum markov games," Proceedings of the Eighteenth Conference on Uncertainty in Artificial Intelligence, 2002.

[17] M. L. Littman, "Markov games as a framework for multi-agent reinforcement learning," Proceedings of the Eleventh International Conference on Machine Learning, 1994.

[18] T. Basar and G.J. Olsder, Dynamic noncooperative game theory, 2nd edition, Society for Industrial and Applied Mathematics, 1995.

[19] T. Raghaven, T. Ferguson, T. Parthasarathy, and O. Vrieze, Stochastic games and related topics, Springer, 1990.

[20] M.L. Puterman, Markov decision processes: discrete stochastic dynamic programming, John Wiley & Sons, New York, 1994.

[21] M. Littman, "Friend-or-foe q-learning in general-sum markov games," In Proceedings of Eighteenth International Conference on Machine Learning, 2001.

[22] H. Li, M. Y. Chow, and Z. Sun, "Optimal stabilizing gain selection for networked control systems with time delays and packet losses," IEEE Transactions on Control Systems Technology, vol. 17, no. 5, September 2009.

[23] H. Xu, S. Jagannathan, and F.L. Lewis, "Stochastic optimal design for unknown linear discrete-time systems zero-sum games in input-output form under communication constraints," Asian Journal of Control, vol. 16, no. 5, pp. 1263-1276, September 2014.

[24] G. Kreisselmeier, "Adaptive control of a class of slowly time-varying plants," System Control Letter, vol. 8, pp. 97-103, June 1986.

[25] J. Yu, Z. Su, M. Wang, M. Tan, and J. Zhang, "Control of yaw and pitch maneuvers of a multilink dolphin robot," IEEE Transactions on Robotics, vol. 28, no. 2, pp. 318-329, 2012.

[26] G. Cai, B.M. Chen, K. Peng, M. Dong, and T.H. Lee, "Modeling and control of the yaw channel of a UAV helicopter," IEEE Transactions on Industrial Electronics, vol. 55, no. 9, pp. 3426-3434, September 2008.

[27] B. Mettler, Identification modeling and characteristics of miniature rotorcraft. Norwell, MA: Kluwer, 2003.

[28] D. H. Shim, H. J. Kim, and S. Sastry, "Control system design for rotorcraft-based unmanned aerial vehicle using time-domain system identification," IEEE Conference on Control Application, 2000.

[29] L. Ljung, System identification—theory for the user, 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 1999.

[30] S. Kumar, "Smurf-based distributed denial of service attack amplification in internet," Internet Monitoring and Protection, 2007.

[31] G. R. Zargar and P. Kabiri, "Identification of effective network features to detect smurf attacks," IEEE Student Conference on Research and Development (SCOReD), 2009.

[32] S. Cai, Y. Liu, and W. Gong, "Client-controlled slow tcp and denial of service," 43rd IEEE Conference on Decision and Control, 2004.

[33] M., Xue, W. Wang, and S. Roy, "Security concepts for the dynamics of autonomous vehicle networks," Automatica, vol. 50, no. 3, pp. 852-857, 2014.

[34] C. W. Chen and S. Roy, "State detection from local measurements in network synchronization processes," International Journal of Control, vol. 86, no. 9, pp. 1634-1645, 2013.

[35] S. Roy, M. Xue, and S. K. Das, "Security and discoverability of spread dynamics in cyber-physical networks," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 9, pp. 1694-1707, 2012.

III. FLOW-BASED ATTACK DETECTION AND ACCOMMODATION FOR NETWORKED CONTROL SYSTEMS

Haifeng Niu and S. Jagannathan

In networked control systems, the communication links are vulnerable to a variety of potential malicious attacks. In this paper, we first propose a novel attack detection scheme that is capable of capturing the abnormality in the traffic flow in those communication links due to a class of attacks. Further, it is shown that the stability of the physical system can be affected by the condition of the network due to delays and packet losses induced by the attacks. An observer-based detection scheme is developed both for the network and physical system. Attacks on the networks as well as on the physical system can be detected and upon detection, the physical system can be stabilized by adjusting the controller gains. Several attacks are considered in the simulation to show the applicability of the proposed scheme.

1. INTRODUCTION

Networked control systems (NCS) are ubiquitous with applications ranging from large-scale industrial systems to critical infrastructure such as electric networks. In NCS, the digital controllers receive measured data from sensors and transmit control commands to the actuators through a communication network. However, the data flow between different system components are vulnerable to a variety of potential system disturbances and malicious attacks, which have been recently discussed and summarized [1].

The defense methodology in NCS can be due to [2]: 1) protection of information in the cyber system and 2) attenuation of disturbances and detection of states abnormalities in the physical system. The majority of the effort in the former category is devoted to the development of encryption algorithms on the communication channel [2]. However, it is only a partial solution for securing NCS because certain attacks, especially those that target information availability such as denial of service (DoS) attacks, do not require the data to be decoded. Moreover, the delay induced by the encryption methods could lead to performance degradation of the control system.

Other effort [3-7] in the former category explore the behavior of the attacker as well as the defender, formulate the cyber changes under attacks, and present an appropriate strategy to bring the cyber system back to normal. For instance, the effort in [3] introduces the Denial of Service (DoS) flooding attacks by a continuous-time Markov chain and utilizes the state space method to compute security measures accurately. Different from [3], the authors in [4] study the cyber defense by modeling the actions of the attacker and the defender as a stochastic zero-sum game. In [5], the measure of vulnerabilities in cyber-physical systems with application to power systems is defined and a security framework

including anomaly detection and mitigation strategies is provided. The authors in [6] evaluate the cyber security by computing the expected probabilities of the attacker and using the probabilities to build a transition model through game-theoretic approach. In [7], the cyber vulnerability is evaluated dynamically by using hidden Markov model and by providing a mechanism for handling sensor data with different trustworthiness.

On the other hand, the latter category concentrates on characterizing the dynamics of the physical system under attacks by extending the classical state-space description. For instance, in [8], the system dynamics include an extra term to model the deception attack. In [9], the system state under attack is represented with an additive term which in turn is used to simulate the false data injection attack. Unlike [9], the authors in [10] characterize the deception attacks using a set of objectives and propose policies to synthesize stealthy deception attacks in both linear and nonlinear estimators.

In [11], the estimation and control of linear systems when sensors or actuators are corrupted by an attacker is provided, together with a secure local control loop that can improve the resilience of the system. On the other hand, the authors in [12] define the control input under attacks as the product of the given input and a coefficient to characterize the effect induced by the DoS attacks. A class of human adversaries, referred to as correlated jammers, is considered in [13]. By modeling the coupled decision making process as a two-level receding-horizon dynamic game, the authors propose a control law and analyze the performance and the closed-loop stability under attacks.

Despite interesting ideas by the above mentioned effort [8-13] for the security of the overall NCS, there are many weaknesses [14]. First, the representation can only describe a single type of attack due to the fact that attacks affect the system dynamics in a

variety of ways. In particular, in [14] a unified framework that is able to detect attacks is proposed whereas it still has the two drawbacks mentioned next. Second, it is difficult to implement the representation developed in the literature so far since the system dynamics under attacks are considered known. For instance, due to random delays and packet losses caused by certain cyber-attacks, the physical system dynamics will become uncertain [15]. This problem has been addressed by the authors [15][16] by using Q-learning and zero-sum game theoretic formulation.

However, the cyber-attacks may not be detected in a timely manner until a significant deviation in the physical system state vector is observed. For instance, it is well-known that a large delay and packet loss rate can result in the instability of the physical system [16]. Instead of waiting for the detection of abnormal state vector in the physical system, it is better to identify the problematic communication link that is likely to be congested with excessive data by the attacks, which is not covered in our previous work [15]. Therefore, in this paper, we propose a detection scheme that is capable of capturing the abnormal traffic flow in the communication links for certain class of cyber-attacks given the network and physical system dynamics under consideration.

We begin by introducing the state–space representation of traffic flow under cyber-attacks with random delayed measurements for the communication network. Next, we derive the observer-based controller that stabilizes the flow during healthy conditions without attacks within the desired level by using linear matrix inequality (LMI) in the presence of delayed information. By using the observer and measured outputs, network attack detection residual is generated which in turn is utilized to determine the onset of an attack in the communication network when the residual exceeds a predefined threshold.

Then the detectability condition is introduced and the performance of the attack detection scheme is discussed.

Next, we introduce an attack detection scheme for the physical system that is capable of detecting attacks in both the communication network and physical system. A new controller gain will be selected upon the detection of attacks in order to stabilize the physical system. Finally the proposed scheme is evaluated by considering four types of cyber-attacks in the simulation. The results verify that the proposed scheme for the networks is able to detect certain types of attacks while revealing inherent limitation. The simulation results on the physical systems verify that the attacks on both the network and the physical system can be detected and the physical system can be stabilized by applying the obtained controller gains. The results of the hardware implementation on an RFID network confirm that both the jamming attack and the blackhole attack can be detected by the proposed detection scheme.

The contributions of the paper include: 1) the design of the flow controller with randomly delayed measurement in the presence of attacks; 2) the development of novel observer-based network attack detection and estimation scheme along with detectability condition; 3) the design of the observer and the detection scheme using measured outputs of the physical system for detecting attacks on both network and the physical system; 4) the controller design for the physical system to maintain the stability of the physical system which can be utilized to maintain the healthy condition of the communication networks in terms of the delays and packet losses; and 5) demonstration of the proposed scheme in both simulation and hardware implementation, in the presence of a class of attacks with specific adversary models.

The rest of this paper is organized as follows. In Section 2, we introduce the state-space stochastic flow model under cyber-attacks. The observer and controller design is presented in Section 3, followed by the adversary model and cyber-attack detectability provided in Section 4. In Section 5 we present the detection scheme and controller design for the physical system. The simulation as well as the hardware implementation results and analysis are given in Section 6 and conclusions in Section 7.

The notations used in the paper are briefly introduced. $Prob\{\cdot\}$ stands for the probability of the event occurring "$\cdot$". $E\{x\}$ denotes the expectation of the stochastic variable x, $\lambda_{\max}\{M\}$ represents the largest eigenvalue of matrix M, $diag\{v\}$ stands for the square diagonal matrix with the elements of vector v (or with the sub-blocks of matrix v) on the main diagonal and the "*" in matrices denotes the symmetric terms.

2. STOCHASTIC FLOW MODEL

Figure 2.1 shows the diagram of a typical NCS, in which both the controller commands and the sensor data are transmitted through a wired or wireless communication link. In this section, we propose a stochastic state-space representation in discrete-time for the traffic flow at the bottleneck link in the presence of attacks. It is verified both theoretically and experimentally [17] that the performance measures such as the delay and transmission rate are determined by the bottleneck node and therefore a mild assumption widely reported in the literature [18][19] is asserted.

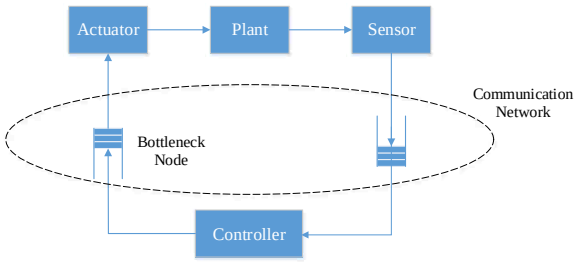


Figure 2.1. Diagram of a typical NCS.

Let the input rate at sampling time kT be $\bar{\mu}_k$ packets per second and u_k be the adjustment from the previous input rate, that is

$$\bar{\mu}_k = \bar{\mu}_{k-1} + u_k \,. \tag{1}$$

The transmission or output rate $\bar{\upsilon}_k$, which slightly fluctuates around the standard transmission rate υ_0, is modeled by a stable autoregressive–moving-average (ARMA) process given by [19]

$$\bar{\upsilon}_k = \upsilon_0 + \delta_k , \tag{2}$$

where

$$\delta_k = \sum_{i=1}^{m} l_i \delta_{k-i} + d_{k-1} , \tag{3}$$

where " d " represents a bounded disturbance with d_M being its bound, l and m are predefined constants obtained during system identification. Compared with other transmission rate models such as the random walk model [19], the advantages with the ARMA process is that it is analytically tractable and capable of capturing a wide range of possible behavior.

Let the traffic flow in the bottleneck node at time kT be $\bar{\rho}_k$. Then we have

$$\bar{\rho}_{k+1} = \bar{\rho}_k + T\bar{\mu}_k - T\bar{\upsilon}_k + \omega_k , \tag{4}$$

where ω_k is the number of the packets introduced by the attacker with $\omega_k > 0$ implies that the attacker has injected data while $\omega_k < 0$ implies that the attacker has dropped data. More detailed representation of the attack models can be found in Section 4.

Let the desired flow at the bottleneck node be ρ_0 and re-write (4) as

$$\bar{\rho}_{k+1} - \rho_0 = (\bar{\rho}_k - \rho_0) + T(\bar{\mu}_k - \nu_0) - T\delta_k + \omega_k . \tag{5}$$

Now define the shifted flow ρ_k and input rate μ_k as

$$\rho_k = \bar{\rho}_k - \rho_0, \mu_k = \bar{\mu}_k - \upsilon_0 . \tag{6}$$

Then the flow dynamic in (5) become

$$\rho_{k+1} = \rho_k + T\mu_k - T\delta_k + \omega_k . \tag{7}$$

Define the state vector $x_k = [\rho_k, \mu_k, \delta_k, \cdots, \delta_{k-m+1}]^T$ [19] and combine (1), (3) and (7) to get

$$\begin{bmatrix} \rho_{k+1} \\ \mu_{k+1} \\ \delta_{k+1} \\ \delta_k \\ \vdots \\ \delta_{k-m+2} \end{bmatrix} = \begin{bmatrix} 1 & T & -T & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & l_1 & \cdots & l_{m-1} & l_m \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \begin{bmatrix} \rho_k \\ \mu_k \\ \delta_k \\ \delta_{k-1} \\ \vdots \\ \delta_{k-m+1} \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} u_k + \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} d_k + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \omega_k \tag{8}$$

or

$$x_{k+1} = \bar{A}x_k + \bar{B}u_k + \bar{D}d_k + \bar{W}\omega_k, \tag{9}$$

where $\bar{A}$, $\bar{B}$, $\bar{D}$ and $\bar{W}$ represent the appropriate dimensioned matrices from (8).

It has been reported in the literature [20] that the network state can be easily measured when the servers at the output queues are Rate Allocating Servers and the transport protocol supports the Packet-Pair probing technique. Therefore, in this paper, the network state described by input rate, output rate, and the current flow in the link are considered accessible. Suppose the current traffic flow in the link and the output rate can be known after a delay of $\alpha_k T$, where $\alpha_k \in \{0,1,\cdots\}$ is a stochastic variable. Define the output vector y as

$$y_k = diag\{\vartheta(\alpha_k), 1, \vartheta(\alpha_k), 1\cdots, 1\} \cdot x_k + \sum_{i=1}^{\alpha_k} diag\{\vartheta(\alpha_k - i), 0, \vartheta(\alpha_k - i), 0, \cdots, 0\} \cdot x_{k-i} \tag{10}$$

where $\vartheta(x) = 1$ for $x = 0$ and $\vartheta(x) = 0$ for other values of x.

Moreover, as illustrated in Figure 2.2, considering the fact that the backward transmission delay is much smaller than the forward delay due to the lack of queuing time, we make the following weak assumption.

Assumption 1 [21]: Assume $\alpha_k \in \{0,1\}$, i.e., the feedback delay for the output rate and buffer length measurement is one sampling interval at most and α_k is a Bernoulli distributed white sequence with

$$\Pr\{\alpha_k = 1\} = E\{\alpha_k\} := \bar{\alpha}. \tag{11}$$

Then the output vector y in (10) becomes

$$\begin{aligned} y_k &= \begin{bmatrix} (1-\alpha_k)\rho_k + \alpha_k \rho_{k-1} \\ \mu_k \\ (1-\alpha_k)\delta_k + \alpha_k \delta_{k-1} \\ \cdots \\ \delta_{k-m+1} \end{bmatrix} \\ &= diag\{(1-\alpha_k),1,(1-\alpha_k),1\cdots,1\} \cdot x_k + diag\{\alpha_k,0,\alpha_k,0,\cdots,0\} \cdot x_{k-1} \end{aligned} \tag{12}$$

Define a diagonal matrix with the random variable α_k as $\Gamma_k \triangleq diag\{\alpha_k,0,\alpha_k,0\cdots,0\}$ and we further let $\bar{\Gamma} \triangleq diag\{\bar{\alpha},0,\bar{\alpha},0,\cdots,0\}$. Then (12) can be re-written as

$$y_k = (I - \Gamma_k)x_k + \Gamma_k x_{k-1}. \tag{13}$$

Now we are ready to introduce the flow observer and controller. Controller will be utilized for the system (9) in the absence of network attacks first.

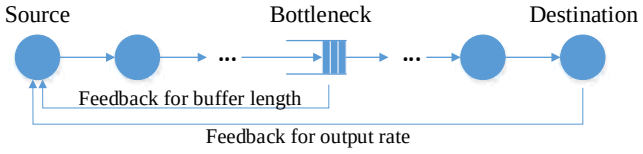


Figure 2.2. Illustration of the delayed measurement.

3. FLOW OBSERVER AND CONTROLLER DESIGN

The benefit of the observer is twofold. On one hand, due to the stochastic delay in measurement, the state cannot be known instantaneously. An estimated state, which is generated by the observer, will be utilized by the controller. On the other hand, by using the measured and estimated outputs, an estimation error or attack residual is generated for detection. The observer is described as

$$\begin{cases} \hat{x}_{k+1} = \bar{A}\hat{x}_k + \bar{B}u_k + L(y_k - \hat{y}_k) \\ \hat{y}_k = (I - \bar{\Gamma}_k)\hat{x}_k + \bar{\Gamma}_k \hat{x}_{k-1} \end{cases}, \tag{14}$$

and the flow controller is given by using the observer state as

$$u_k = K\hat{x}_k, \tag{15}$$

where L and K denote the observer and controller gain matrices, respectively, with appropriate dimension to be designed later.

Define the state estimation error as

$$e_k = x_k - \hat{x}_k . \tag{16}$$

Then the state and the estimation error dynamics become

$$x_{k+1} = \left(\bar{A} + \bar{B}K\right)x_k - \bar{B}Ke_k + \bar{D}d_k + \bar{W}\omega_k , \tag{17}$$

$$e_{k+1} = L(\Gamma - \bar{\Gamma})x_k + \left[\bar{A} - L\left(I - \bar{\Gamma}\right)\right]e_k - L\left(\Gamma - \bar{\Gamma}\right)x_{k-1} - L\bar{\Gamma}e_{k-1} + \bar{D}d_k + \bar{W}\omega_k . \tag{18}$$

Combining (17) and (18) yields

$$\begin{bmatrix} x_{k+1} \\ e_{k+1} \\ x_k \\ e_k \end{bmatrix} = \begin{bmatrix} \bar{A} + \bar{B}K & -\bar{B}K & \mathbf{0} & \mathbf{0} \\ L(\Gamma - \bar{\Gamma}) & \bar{A} - L\left(I - \bar{\Gamma}\right) & -L\left(\Gamma - \bar{\Gamma}\right) & -L\bar{\Gamma} \\ I & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I & \mathbf{0} & \mathbf{0} \end{bmatrix} \begin{bmatrix} x_k \\ e_k \\ x_{k-1} \\ e_{k-1} \end{bmatrix} + \begin{bmatrix} \bar{D} \\ \bar{D} \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix} d_k + \begin{bmatrix} \bar{W} \\ \bar{W} \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix} \omega_k . \tag{19}$$

Now define the augmented state vector as $X_k = [x_k \quad e_k \quad x_{k-1} \quad e_{k-1}]^T$. Then (19) becomes

$$X_{k+1} = AX_k + Dd_k + W\omega_k, \tag{20}$$

where A, D, and W represent system matrices from (20).

Next we will first introduce the definition of stochastic stability in the mean-square sense together with the H_∞ performance constraints since the closed-loop dynamic system of the source-destination pair described in (20) contains stochastic variable Γ. Then we will introduce the design of the controller and observer gain matrices L and K such that the system (20) is stabilized and satisfies the H_∞ performance constraints in the absence of attacks. We solve the gain matrices L and K by using linear matrix inequalities (LMI). Finally, we will demonstrate that with the obtained L and K, the estimation error is bounded when the attacks are absent.

3.1. STABILITY IN THE HEALTHY CASE

Before obtaining the gain matrices, the following definitions and lemmas are needed in order to proceed.

Definition 1 [21]: The closed-loop system (20) is said to be exponentially mean-square stable with $d_k = 0$ and $\omega_k = 0$, if there are constants $\partial > 0$ and $\tau \in (0,1)$ such that

$$E\left\{\|X_k\|^2\right\} \le \partial \tau^k E\left\{\|X_0\|^2\right\}. \tag{21}$$

Before we introduce the theorem on stability in the absence of attacks, the following definition and lemmas are needed.

Definition 2 [22]: The closed-loop system (20) in the absence of attacks meets the H_∞ performance constraints when its state satisfies

$$\sum_{k=0}^{\infty} E\left\{\left\|\bar{G}X_k\right\|^2\right\} < \gamma^2 \sum_{k=0}^{\infty} E\left\{\left\|d_k\right\|^2\right\} \tag{22}$$

for all nonzero d_k, where γ is a prescribed positive scalar, $\bar{G}$ is the given input-output gain matrix.

Lemma 1 [23]: Let $V(X_k)$ be a Lyapunov function for the system (20). If there exists real scalars $\theta_1 > 0$, $\theta_2 > 0$, $\lambda \geq 0$ and $0 < \chi < 1$ such that

$$\theta_1 \left\|X_k\right\|^2 \leq V(X_k) \leq \theta_2 \left\|X_k\right\|^2, \tag{23}$$

and

$$E\left\{V(X_{k+1}) \mid X_k\right\} - \chi V(X_k) \leq \lambda, \tag{24}$$

then the sequence X_k satisfies

$$E\left\{\left\|X_k\right\|^2\right\} \leq \frac{\theta_2}{\theta_1}\left\|X_0\right\|^2 \chi^k + \frac{\lambda}{\theta_1(1-\chi)}. \tag{25}$$

Lemma 2 [24]: Let A be a real $n \times n$ matrix and $B = diag\{b_1, \cdots b_n\}$ be a diagonal stochastic matrix. Then

$$E\left\{BAB^T\right\} = \begin{bmatrix} E\left\{b_1^2\right\} & \cdots & E\{b_1 b_n\} \\ \vdots & \ddots & \vdots \\ E\{b_n b_1\} & \cdots & E\left\{b_n^2\right\} \end{bmatrix} \otimes A,$$

where $\otimes$ is the Hadamard product, i.e., $[A \otimes B]_{ij} = A_{ij} \cdot B_{ij}$.

Lemma 3 (Schur Complement): Let matrix $M = \begin{bmatrix} M_1 & M_2 \\ M_2^T & M_3 \end{bmatrix}$ where M_1, M_2, and M_3 are matrices with appropriate dimensions. Then M is positive definite (PD) if and only if both M_3 and matrix $\left(M_1 - M_2 M_3^{-1} M_2^T\right)$ are PD.

Lemma 4: For a given observer gain matrix L and controller gain matrix K, the closed-loop system (20) is exponentially mean-square stable in the absence of disturbances and attacks if there exist positive definite matrices P_1, P_2, P_3, and P_4, such that

$$\begin{bmatrix} Q_2 & Q_1^T \\ Q_1 & -Q_3^{-1} \end{bmatrix} < 0, \tag{26}$$

where $Q_1 \sim Q_3$ are defined as

$$Q_1 = \begin{bmatrix} \bar{A}+\bar{B}K & -\bar{B}K & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \bar{A}-L\left(I-\bar{\Gamma}\right) & \mathbf{0} & -L\bar{\Gamma} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ L\tilde{\Gamma} & \mathbf{0} & -L\tilde{\Gamma} & \mathbf{0} \end{bmatrix} \triangleq \begin{bmatrix} Q_{11} \\ Q_{12} \\ Q_{13} \\ Q_{14} \end{bmatrix}, \tag{27}$$

where $\tilde{\Gamma} = diag\left\{\sqrt{\bar{\alpha}(1-\bar{\alpha})}, 0, \sqrt{\bar{\alpha}(1-\bar{\alpha})}, 0, ..., 0\right\}$,

$$Q_2 = diag\left\{P_2 - P_1, P_4 - P_3, -P_2, -P_4\right\}, \tag{28}$$

and

$$Q_3 = diag\left\{P_1, P_3, P_1, P_3\right\}, \tag{29}$$

Proof: Let the Lyapunov function be defined as

$$V_k = x_k^T P_1 x_k + x_{k-1}^T P_2 x_{k-1} + e_k^T P_3 e_k + e_{k-1}^T P_4 e_{k-1}, \tag{30}$$

where P_1, P_2, P_3, and P_4 are PD matrices. For the rest of the paper, we let $V_k \triangleq V(x_k)$ for short.

Then from (17) and (18) it follows that

$$\begin{aligned} & E\{V_{k+1}\} - V_k \\ & = E\left\{x_{k+1}^T P_1 x_{k+1} + e_{k+1}^T P_3 e_{k+1}\right\} + x_k^T P_2 x_k + e_k^T P_4 e_k - x_k^T P_1 x_k - x_{k-1}^T P_2 x_{k-1} - e_k^T P_3 e_k - e_{k-1}^T P_4 e_{k-1} \\ & = \left(\left(\bar{A}+\bar{B}K\right)x_k - \bar{B}Ke_k\right)^T P_1 \left(\left(\bar{A}+\bar{B}K\right)x_k - \bar{B}Ke_k\right) \\ & + \left(\left(\bar{A}-L\left(I-\bar{\Gamma}\right)\right)e_k - L\bar{\Gamma}e_{k-1}\right)^T P_3 \left(\left(\bar{A}-L\left(I-\bar{\Gamma}\right)\right)e_k - L\bar{\Gamma}e_{k-1}\right) \\ & + E\left\{\left(L\left(\Gamma-\bar{\Gamma}\right)\left(x_k - x_{k-1}\right)\right)^T P_3 \left(L\left(\Gamma-\bar{\Gamma}\right)\left(x_k - x_{k-1}\right)\right)\right\} \\ & + x_k^T P_2 x_k + e_k^T P_4 e_k - x_k^T P_1 x_k - x_{k-1}^T P_2 x_{k-1} - e_k^T P_3 e_k - e_{k-1}^T P_4 e_{k-1} \end{aligned} . \tag{31}$$

Applying Lemma 2, we have

$$\begin{aligned} & E\left\{\left(x_k - x_{k-1}\right)^T \left(L\left(\Gamma - \bar{\Gamma}\right)\right)^T P_3 \left(L\left(\Gamma - \bar{\Gamma}\right)\right)\left(x_k - x_{k-1}\right)\right\} \\ &= \left(x_k - x_{k-1}\right)^T E\left\{\left(\Gamma - \bar{\Gamma}\right)^T L^T P_3 L\left(\Gamma - \bar{\Gamma}\right)\right\}\left(x_k - x_{k-1}\right) \\ &= \left(Lx_k - Lx_{k-1}\right)^T \cdot \bar{\Gamma}\left(I - \bar{\Gamma}\right) P_3 \cdot \left(Lx_k - Lx_{k-1}\right) \\ &= \left(L\tilde{\Gamma}x_k - L\tilde{\Gamma}x_{k-1}\right)^T P_3 \left(L\tilde{\Gamma}x_k - L\tilde{\Gamma}x_{k-1}\right). \end{aligned} \tag{32}$$

Substitute (32) into (31), it follows that

$$E\left\{V_{k+1}\right\} - V_k = X_k^T \left(Q_1^T Q_3 Q_1 + Q_2\right) X_k \triangleq X_k^T \Xi X_k \,. \tag{33}$$

Therefore, according to Lemma 3, we have

$$E\left\{V_{k+1}\right\} - V_k = X_k^T \Xi X_k \le -\alpha_1 X_k^T X_k \le -\frac{\alpha_1}{\lambda_{\max}\left\{P\right\}} V_k \,, \tag{34}$$

where $P \triangleq diag\left\{P_1, P_3, P_2, P_4\right\}$ and

$$0 < \alpha_1 < \min\left\{\lambda_{\min}\left\{-\Xi\right\}, \lambda_{\max}\left\{P\right\}\right\}. \tag{34}$$

Thus, (34) together with Lemma 1 completes the proof.

Next, Theorem 1 introduces the selection of controller and observer gain matrices L and K in order to both stabilize the system and meet the performance constraints.

Theorem 1: Given a positive scalar γ_1, the system (20) without attacks i.e. $\omega_k = 0$, is exponentially mean-square stable and satisfies the H_∞ performance constraint, if there exist real matrices L, K and positive definite matrices P_1, P_2, P_3, and P_4 satisfying

$$\begin{bmatrix} S_2 & S_1^T \\ S_1 & -S_3^{-1} \end{bmatrix} < 0 \,. \tag{36}$$

with S_1, S_2, and S_3 defined as

$$S_1 = \begin{bmatrix} Q_1 & D \\ G & \mathbf{0} \end{bmatrix} \text{ where } G = \begin{bmatrix} \bar{G} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}, \tag{37}$$

$$S_2 = diag\left\{Q_2, -\gamma_1^2 I\right\}, \tag{38}$$

$$\text{and } S_3 = diag\left\{Q_3, I\right\}. \tag{39}$$

Proof: It is clear that (35) implies (25), and by Lemma 4, it follows that the system is exponentially mean-square stable. Now consider the following term

$$\begin{aligned} &E\{V_{k+1}\} - E\{V_k\} + E\left\{\left(\bar{G}x_k\right)^T\left(\bar{G}x_k\right)\right\} - \gamma_1^2 E\left\{d_k^T d_k\right\} \\ &= E\left\{V_{k+1} - V_k + x_k^T \bar{G}^T \bar{G} x_k - \gamma_1^2 d_k^T d_k\right\} = E\{X_k^T \Xi X_k + \left(\bar{D}d_k\right)^T P_1 Q_{11} X + \left(Q_{11}X\right)^T P_1\left(\bar{D}d_k\right) \\ &+ \left(\bar{D}d_k\right)^T{}_1 P_1\left(\bar{D}d_k\right) + \left(\bar{D}d_k\right)^T P_3 Q_{12} X + \left(Q_{12}X\right)^T P_3\left(\bar{D}d_k\right) \\ &+ \left(\bar{D}d_k\right)^T{}_1 P_3\left(\bar{D}d_k\right) + x_k^T \bar{G}^T \bar{G} x_k - \gamma_1^2 d_k^T d_{kk}\} \triangleq E\left\{\begin{bmatrix} X \\ d_k \end{bmatrix}^T \Delta \begin{bmatrix} X \\ d_k \end{bmatrix}\right\} \end{aligned} \tag{40}$$

where $\Delta = \begin{bmatrix} \Xi + G^T G & \left(\bar{D}^T P_1 Q_{11} + \bar{D}^T P_3 Q_{12}\right)^T \\ \bar{D}^T P_1 Q_{11} + \bar{D}^T P_3 Q_{12} & \bar{D}^T\left(P_1 + P_3\right)\bar{D} - \gamma_1^2 I \end{bmatrix}$.

Now we are left to prove $\Delta < 0$ where

$$\begin{aligned} \Delta &= diag\left\{Q_2, -\gamma_1^2 I\right\} + \begin{bmatrix} Q_1{}^T Q_3 Q_1 + G^T G & \left(D^T Q_3 Q_1\right)^T \\ D^T Q_3 Q_1 & D^T Q_3 D \end{bmatrix} \\ &= diag\left\{Q_2, -\gamma_1^2 I\right\} + \begin{bmatrix} Q_1 & D \\ G & \mathbf{0} \end{bmatrix}^T \begin{bmatrix} Q_3 & \\ & I \end{bmatrix} \begin{bmatrix} Q_1 & D \\ G & \mathbf{0} \end{bmatrix} = S_2 + S_1^T S_3 S_1 \end{aligned} \tag{41}$$

According to Lemma 3, (36) implies (41). Therefore, we have

$$E\left\{V_{k+1}\right\} - E\left\{V_k\right\} + E\left\{\left(\bar{G}x_k\right)^T\left(\bar{G}x_k\right)\right\} - \gamma_1^2 E\left\{d_k^T d_k\right\} < 0. \tag{42}$$

By summing up (42) from 0 to ∞ with respect to k, it follows that

$$\sum_{k=0}^{\infty} E\left\{\left\|\bar{G}X_k\right\|^2\right\} < \gamma_1^2 \sum_{k=0}^{\infty} E\left\{\left\|d_k\right\|^2\right\} - E\left\{V_\infty\right\}. \tag{43}$$

Since the system is exponentially mean-square stable, inequality (43) becomes

$$\sum_{k=0}^{\infty} E\left\{\left\|\bar{G}X_k\right\|^2\right\} < \gamma_1^2 \sum_{k=0}^{\infty} E\left\{\left\|d_k\right\|^2\right\}. \tag{44}$$

So far we have shown in the absence of attacks, the closed-loop system (20) is exponentially mean-square stable and satisfies the H_∞ performance constraint, as long as the matrices L, K and matrices P_1, P_2, P_3, and P_4 satisfy inequality (36). Therefore now we are at the stage to solve for such matrices, which are presented in the next section.

3.2. CONTROLLER AND OBSERVER GAIN SELECTION

It is important to note that inequality (36) in Theorem 1 is not in the form of LMI due to the term S_3^{-1} and thus cannot be solved directly. The following theorem from [21][25] converts (36) into a solvable LMI and provides the controller and observer gain matrices to stabilize the system while satisfying the H_∞ performance constraints.

Theorem 2 [21][25]: Given positive scalars γ_1 and γ_2, the system (20) is exponentially mean-square stable and satisfies the H_∞ performance constraint, if there exist real matrices M_1, M_2 and PD matrices P_{11}, P_{12}, P_2, P_3,and P_4 satisfying the following LMI

$$\begin{bmatrix} S_2 & \bar{S}_1^T \\ \bar{S}_1 & -\bar{S}_3 \end{bmatrix} < 0, \tag{45}$$

where $\bar{S}_3 = diag\{P_1, P_3, P_1, \tilde{\Gamma}, I\}$, S_2 is defined by (38),

$$S_1^T = \begin{bmatrix} P_1\bar{A}+\bar{B}M_1 & -\bar{B}M_1 & \mathbf{0} & \mathbf{0} & P_1\bar{D} & P_1\bar{W} \\ \mathbf{0} & P_3\bar{A}-M_2(I-\bar{\Gamma}) & \mathbf{0} & -M_2\bar{\Gamma} & P_3\bar{D} & P_3\bar{W} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \tilde{\Gamma}M_2 & \mathbf{0} & -\tilde{\Gamma}M_2 & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \bar{G} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix},$$

$P_1 = U^T diag\{P_{11}, P_{12}\}U$ and $U = diag\{[0,1;-1;0], diag\{1,...,1\}\}$.

Moreover, the controller and observer gain matrices are given by

$$K = P_{11}^{-1}M_1 \text{ and } L = P_3^{-1}M_2. \tag{46}$$

The proof is similar to that of ([21], Theorem 3) and thus omitted. Next, the following corollary verifies that with the controller and observer gain matrices generated by Theorem 2, the states of closed-loop system (20) are bounded in the presence of bounded disturbances without any attacks.

Corollary 1: Consider the closed-loop system (20) with the disturbance bounded by d_M in the absence of attacks i.e. $\omega_k = 0$. Let the controller and observer gain matrices be generated by Theorem 2, then the estimation error is bounded in the mean square such that

$$E\left\{\left\|e_k\right\|^2\right\} \le \Upsilon, \tag{47}$$

with

$$\Upsilon \triangleq \frac{\lambda_{\max}\{P\}}{\lambda_{\min}\{P\}}\left(\left\|X_0\right\|^2 + \frac{\left\|\alpha_2^{-1} + D^T Q_3 D\right\| d_M^2}{-\lambda_{\min}\{-\Xi\} + \alpha_2 \lambda_{\max}\{\Lambda\}}\right), \tag{48}$$

where $\Lambda \triangleq \left(D^T Q_3 Q_1\right)^T \left(D^T Q_3 Q_1\right)$ and α_2 is a positive real number satisfying

$$-\lambda_{\min}\{P\} < -\lambda_{\min}\{-\Xi\} + \alpha_2 \lambda_{\max}\{\Lambda\} < 0. \tag{49}$$

Proof: Select the Lyapunov function defined in (30) and combine the system dynamics (20) yields

$$\begin{aligned} E\{V_{k+1}\} - V_k &= \begin{bmatrix} X_k^T \\ d_k \end{bmatrix}^T \begin{bmatrix} \Xi & Q_1^T Q_3^T D \\ D^T Q_3 Q_1 & D^T Q_3 D \end{bmatrix} \begin{bmatrix} X_k^T \\ d_k \end{bmatrix} \\ &= X_k^T \Xi X_k + 2 D^T Q_3 Q_1 X_k d_k + D^T Q_3 D d_k^2 \\ &\le X_k^T \Xi X_k + \alpha_2 X_k^T \left(D^T Q_3 Q_1\right)^T \left(D^T Q_3 Q_1\right) X_k + \left(\alpha_2^{-1} + D^T Q_3 D\right) d_k^2 \\ &\le X_k^T \Xi X_k + \alpha_2 X_k^T \left(D^T Q_3 Q_1\right)^T \left(D^T Q_3 Q_1\right) X_k + \left(\alpha_2^{-1} + D^T Q_3 D\right) d_k^2 \\ &\le \left(-\lambda_{\min}\{-\Xi\} + \alpha_2 \lambda_{\max}\{\Lambda\}\right) \left\|X_k\right\|^2 + \left\|\alpha_2^{-1} + D^T Q_3 D\right\| d_M^2. \end{aligned} \tag{50}$$

By further applying (49) in (50) we have

$$E\{V_{k+1}\} \le \left(1 - \frac{-\lambda_{\min}\{-\Xi\} + \alpha_2 \lambda_{\max}\{\Lambda\}}{\lambda_{\max}\{P\}}\right) V_k + \left\|\alpha_2^{-1} + D^T Q_3 D\right\| d_M^2. \tag{51}$$

Next apply Lemma 1 to (51) to obtain

$$E\left\{\|X_k\|^2\right\} \le \frac{\lambda_{\max}\{P\}}{\lambda_{\min}\{P\}}\|X_0\|^2\left(1-\frac{-\lambda_{\min}\{-\Xi\}+\alpha_2\lambda_{\max}\{\Lambda\}}{\lambda_{\max}\{P\}}\right)^k + \frac{\lambda_{\max}\{P\}}{\lambda_{\min}\{P\}}\frac{\left\|\alpha_2^{-1}+D^TQ_3D\right\|d_M^2}{-\lambda_{\min}\{-\Xi\}+\alpha_2\lambda_{\max}\{\Lambda\}}. \quad (52)$$

Therefore it follows that

$$E\left\{\|e_k\|^2\right\} \le E\left\{\|X_k\|^2\right\} \le \Upsilon. \quad (53)$$

Remark 1: Corollary 1 introduces the bound of the estimation error when there is no attack and can be utilized to design an attack detection scheme when the estimation exceeds this bound. With the presence of bounded attacks, $\|\omega_k\| \le \omega_M$, by following the same procedure, one can show that the estimation error is also bounded with $E\left\{\|e_k\|^2\right\} \le \Upsilon'$ where $\Upsilon' > \Upsilon$.

4. NETWORK ATTACK DETECTION

In this section, we first introduce the adversary models of three typical flow-targeted network attacks. Next, we develop the network attack scheme based on the observer designed in the previous section. The detectability condition is also given under which certain types of attacks can be detected.

4.1. ADVERSARY MODEL

Cyber-attacks are multifarious but they all target at one or more of the three fundamental properties of information and services: confidentiality, integrity, and availability, often known as CIA [26]. Confidentiality-targeted attacks are usually defended by encryption techniques and therefore in this paper, we only concern about attacks that impair the integrity and availability. Specifically, in the context of flow management, this paper deals with attacks that either inject false data or drop/block authentic data. Three types of such attacks are considered as examples.

Jamming Attack: The jamming attacker aims at creating traffic congestion by placing jammers that consistently inject data into the link. Assuming the attacking strength (number of jammers) increases linearly, then this type of attack can be modeled by [27]

$$\omega_k = 1 - e^{-\beta k}, \tag{54}$$

where k, ω_k and β is the time, percentage of injected data, and the network-related coefficient, respectively. Jamming attack is plotted in Figure 4.1.

Black hole Attack: If the attacker manages to compromise one or more nodes in the routing path from the source to the destination, then a black hole attack has been launched. As a result, part of the data (depending on the attack strength) would be discarded.

Assuming the attack strength (number of black holes) increases linearly, then the black hole attack can be modeled by a linear equation [28] given by

$$\omega_k = 1 - \beta k \,, \tag{55}$$

where k, ω_k and β is the attack strength (number of black holes), percentage of dropped data, and the network-related coefficient, respectively and it is plotted in Figure 4.2.

Minimum Rate DoS Streams Attack: Instead of continuously injecting data, false data is periodically injected into the network, in order to avoid router-based mechanisms that detect high rate flows. In this way, the attacker attempts to minimize their exposure to detection mechanisms. A typical minimum rate DoS stream attack is described by [29]

$$\omega_k = \begin{cases} n_1, & \text{for } t \in \left[k\tilde{T}, k\tilde{T} + p_1 \right] \\ n_2, & \text{for } t \in \left[k\tilde{T} + p_1, k\tilde{T} + p_2 \right] \\ 0, & \text{for } t \in \left[k\tilde{T} + p_2, (k+1)\tilde{T} \right] \end{cases}, \tag{56}$$

where n_1, n_2, η, p_1, p_2 ,and $\tilde{T}$ is the first attack strength, second attack strength, packet drop rate, first attack duration, second attack end time, and total attack period, respectively. The DOS stream attack is plotted in Figure 4.3. Next, an attack detection scheme is introduced.

4.2. ATTACK DETECTION SCHEME

In this section, we will present the attack detectability condition followed by the detection scheme performance.

Theorem 3 (Attack Detectability Condition): Consider the closed-loop system (20) with the disturbance bound d_M . Let the controller and observer gain matrices be generated by using Theorem 2. Attacks can be detected if the injected (dropped) traffic flow ω_k into (from) the link satisfies

$$\left\| \sum_{i=0}^{k-1} \Phi(k,i+1) W \omega_i \right\| > \Upsilon + \sum_{i=0}^{k-1} \left\| \Phi(k,i+1) D d_M \right\| \ , \tag{57}$$

where $\Phi(m,n) = \begin{cases} A(m-1)\cdots A(n), & \text{if } m > n \\ I, & \text{if } m = n \end{cases}$. (58)

Proof: The solution for closed-loop system (20) is given by

$$X_k = \sum_{i=0}^{k-1} \Phi(k,i+1)\left(D d_i + W \omega_i \right) \ , \tag{59}$$

If (57) is satisfied, by using triangle inequality we have

$$\begin{aligned} \| X_k \| &\geq \left\| \sum_{i=0}^{k-1} \Phi(k,i+1) W \omega_i \right\| - \left\| \sum_{i=0}^{k-1} \Phi(k,i+1) D d_i \right\| \\ &> \Upsilon + \sum_{i=0}^{k-1} \left\| \Phi(k,i+1) D d_M \right\| - \sum_{i=0}^{k-1} \left\| \Phi(k,i+1) D d_M \right\| = \Upsilon \end{aligned} \tag{60}$$

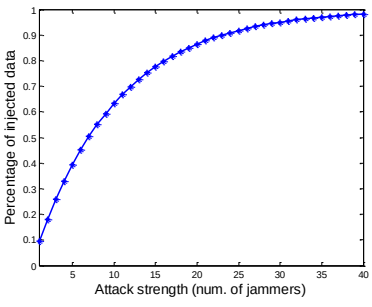


Figure 4.1. Jamming attack.

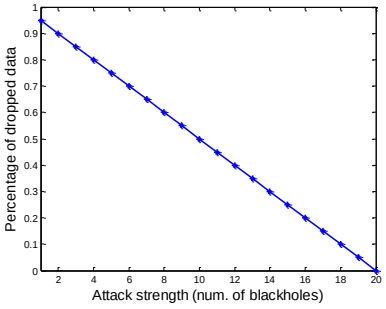


Figure 4.2. Black hole attack.

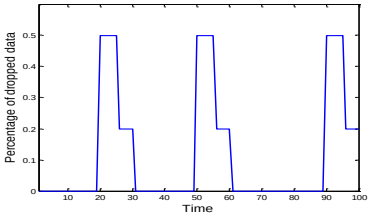


Figure 4.3. Minimum rate DoS streams attack.

Note that the inequality (57) presents a sufficient condition under which certain types of attacks can be detected. However it is not the way how the attack is detected in practice. Instead, the estimation error or the detection residue is constantly monitored and

the attack is detected when the residue exceeds the bound given by (44). Moreover, since the accumulated value of attack function ω_k is used in (57), it is possible that certain attacks cannot be detected, which will be further demonstrated in Section 6.

Combining Corollary 1 and Theorem 3, we are now ready to introduce the main results for the proposed attack detection scheme.

Theorem 4: Consider the closed-loop system (20) with the disturbance bound d_M and the controller and observer gain matrices generated by Theorem 2. The attacks can be detected when the network detection residual exceeds a predefined threshold given by (48) provided $\|\omega_k\| \le \omega_M$. Upon detecting the attack, consider the observer

$$\hat{x}_k = \bar{A}\hat{x}_{k-1} + \bar{B}u_{k-1} + \bar{W}\hat{\omega}_{k-1} - \hat{A}e_{k-1}, \tag{61}$$

to estimate the attack flow where $\hat{\omega}_k$ is the estimated attack flow which is updated using

$$\hat{\omega}_k = \hat{\omega}_{k-1} + \alpha_3 \bar{K} e_{k-1} \bar{A}^T \bar{W} - \alpha_4 \left| 1 - \alpha_3 \bar{W}^T \bar{W} \right| \hat{\omega}_{k-1}, \tag{62}$$

with $\alpha_3, \alpha_4 \in \mathbb{R}$ and $\hat{A}, \bar{K} \in \mathbb{R}^{(m+2)\times(m+2)}$ are design parameters. Then the network attack residual e_k and the estimation error of the attacking flow $\tilde{\omega}_k$ are bounded.

Proof: Select the Lyapunov function candidate as

$$V = V_1 + V_2 \text{ where } V_1 = \frac{1}{3} e_k^T e_k \text{ and } V_2 = \alpha_3^{-1} \tilde{\omega}_k^2 \tag{63}$$

From (61) we can have the estimation error dynamics given by

$$e_k = A_0 e_{k-1} + \bar{W}\tilde{\omega}_{k-1} + \bar{D}d_{k-1}\ , \tag{64}$$

where $A_0 = \bar{A} - \hat{A}$. Substitute (61) and (64) into (63), we have

$$\begin{aligned} &E\left\{V_1(k) \,|\, V_1(k-1)\right\} \\ &= 1/\left(3e_k^T e_k\right) - 1/\left(3e_{k-1}^T e_{k-1}\right) \le e_{k-1}^T A_0^T A_0 e_{k-1} + \bar{W}^T \bar{W} \tilde{\omega}_{k-1}^2 + d_{k-1}^T \bar{D}^T D d_{k-1} - 1/\left(3e_{k-1}^T e_{k-1}\right) \end{aligned}$$

$$\begin{aligned} & E\left\{V_2(k)\,|\,V_2\left(k-1\right)\right\} \\ & = \alpha_3^{-1}\left(\tilde{\omega}_k^2 - \tilde{\omega}_{k-1}^2\right) \\ & \le \frac{2}{\alpha_3}\tilde{\omega}_{k-1}^2 - \frac{6}{\alpha_3}\alpha_5\tilde{\omega}_{k-1}^2 + \frac{3}{\alpha_3}\alpha_5^2\left(\tilde{\omega}_{k-1}^2 + \omega_{k-1}^2\right) + 3\alpha_3\bar{W}^T A_0 e_{k-1}\bar{K}^T\bar{K}e_{k-1}^T A_0^T\bar{W} \end{aligned}, \tag{65}$$

where $\alpha_5 = \alpha_4\left|1-\alpha_3\bar{W}^T\bar{W}\right|\hat{\omega}_{k-1}$. Combing (64) and (65) and after manipulation, we have

$$\begin{aligned} & E\left\{V\left(k\right)|V\left(k-1\right)\right\} \\ & \le -\left[\frac{1}{3} - \lambda_{\max}^2\left\{A_0\right\}\left(1+3\alpha_3\left(k-1\right)^2\right)\right]e_{k-1}^T e_{k-1} - \left[\alpha_3^{-1}\left(-2+6\alpha_5-3\alpha_5^2\right)-1\right]\tilde{\omega}_{k-1}^2 + \lambda_d^2 d_M^2 + 2\alpha_3^{-1}\alpha_5^2\omega_M^2 \end{aligned}. \tag{66}$$

Therefore, both the network attack residual e_k and the attack flow estimation error $\tilde{\omega}_k$ are bounded by selecting the appropriate design parameters.

Theorem 5 provides a way to estimate the injected or dropped flow by the attacker, which can be further utilized to tune the controller parameters of the physical system. Next, the effect of network attacks on the physical system will be discussed.

5. PHYSICAL SYSTEM CONTROLLER DESIGN

Consider the physical plant with the system dynamics described by

$$\begin{aligned} x_{p,k+1} &= A_p x_{p,k} + B_p u_{p,k} + D_p d_{p,k} + W_p \omega_{p,k} \\ y_{p,k} &= C_p x_{p,k} \end{aligned}, \tag{67}$$

where $x_{p,k}$, $y_{p,k}$, $u_{p,k}$, $d_{p,k}$, and $\omega_{p,k}$ is the system state, output, input, disturbance, and attack respectively. The subscript "p", stands for "physical system", is utilized to differentiate the network system dynamics variables in (9).

Remark 2: Although it appears from (67) that the attack affects the system state dynamics, this representation is not limited to the case where the attack targets the states. For instance, for any actuator attacks, the controller input is manipulated from u_p to u'_p and the dynamics (67) can still be used with the attack term $W_p \omega_{p,k} = B_p \left(u'_p - u_p \right)$.

Let $\tau_{sc}, \tau_{ca} \in \mathbb{Z}$ be the number of sampling cycles to represent the sensor-to-controller and controller-to-actuator delay information and let γ_{pd} be the number of dropped packets. Assume that if the packets containing control and state information are delayed or lost, the most recent values will be used. Under this situation, the state feedback control input and output becomes

$$\begin{aligned} u_{p,k} &= K_p x_{p,k-\tau_{sc}-\tau_{ca}-\gamma_{pd}} \\ y_{p,k} &= C_p x_{p,k-\tau_{sc}-\gamma_{pd}} \end{aligned}. \tag{68}$$

Define $\varepsilon_{p,k} \triangleq \tau_{sc} + \tau_{ca} + \gamma_{pd}$ and $\varepsilon'_{p,k} \triangleq \tau_{sc} + \gamma_{pd}$. Then as illustrated in Figure 5.1, this variable will be used to assess the condition of the communication network, which further determines the controller gain of the physical system. Suppose that in the absence of any attacks on the communication networks, the delay and packet losses are bounded by

$\varepsilon_{p,k} \leq \varepsilon_{M1}$. The term $\varepsilon_{p,k}$ will continue to increase and exceeds ε_{M1} if the attack has been launched yet not detected while $\varepsilon_{p,k}$ will decrease back to normal provided that the attack is defended successfully or on the other hand, it could keep increasing and finally exceed ε_{M2}, which is the maximum allowed value the physical system can tolerate before it can become unstable.

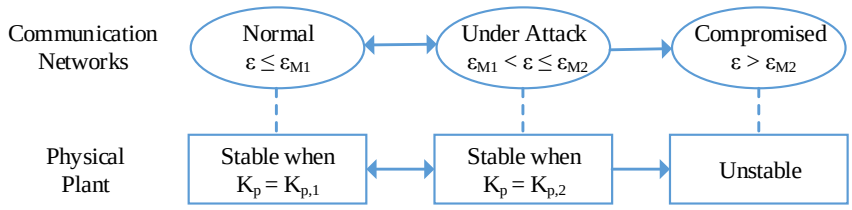


Figure 5.1. Illustration of transitions of the networks and physical states.

For the physical system, the controller gain should be re-configured once an attack on the networks or an abnormity of $\varepsilon_{p,k}$ is detected in order to keep the system stable. For example, suppose $K_{p,1}$ is the controller gain that stabilizes the system for $\varepsilon_{p,k} \leq \varepsilon_{M1}$. Then a different control gain, $K_{p,2}$, needs to be selected once an attack is launched until $\varepsilon_{M1} \leq \varepsilon_{p,k} \leq \varepsilon_{M2}$ beyond which the system becomes unstable. Next this result is stated in the Lemma.

Lemma 5: Let $\varepsilon_{p,k}$ be the networked induced overall delay and packet loss as defined by (68). Let ε_{M1} be the bound of $\varepsilon_{p,k}$ in the absence of network attacks. The closed-loop system (67) in the absence of attacks, i.e., $\omega_{p,k}=0$, on the physical system is stable and satisfies the H_∞ performance constraint $\sum_{k=0}^{\infty}\left\|G_p x_{p,k}\right\|^2 < \gamma_2^2 \sum_{k=0}^{\infty}\left\|d_{p,k}\right\|^2$ for a given positive scalar γ_2, if there exist a real matrix M_3 and PD matrices P_5 and P_6 satisfying

$$\begin{bmatrix} -P_5+\varepsilon_M P_6 & \mathbf{0} & \mathbf{0} & A_p^T P_5^T & G_p^T \\ * & -P_6 & \mathbf{0} & M_3^T & \mathbf{0} \\ * & * & -\gamma_2^2 I & D_p^T P_5^T & \mathbf{0} \\ * & * & * & -P_5 & \mathbf{0} \\ * & * & * & * & -I \end{bmatrix} < 0 . \tag{69}$$

with $\varepsilon_M=\varepsilon_{M1}$. Moreover, the controller gain $K_{p,1}$ for the case of $\varepsilon_{p,k}\le\varepsilon_{M1}$ is given by solving

$$P_5 B_p K_{p,1} = M_3 . \tag{70}$$

However, the stability of the system for this controller gain $K_{p,1}$ cannot be guaranteed if $\varepsilon_{p,k}>\varepsilon_{M1}$.

Proof: Substituting (68) into (67) yields the closed-loop system dynamics:

$$x_{p,k+1} = A_p x_{p,k} + B_p K_p x_{p,k-\varepsilon_{p,k}} + D_p d_{p,k} + W_p \omega_p . \tag{71}$$

Define the Lyapunov function as

$$V_k = x_{p,k}^T P_5 x_{p,k} + \sum_{i=1}^{\varepsilon_{M1}} \sum_{j=k-i}^{k-1} x_{p,j}^T P_6 x_{p,j} \ , \tag{72}$$

where P_5 and P_6 are PD matrices with appropriate dimensions. With the absence of disturbances, the system (71) is stable provided the following inequality holds

$$\Delta V_k = V_{k+1}\left(x_p\right) - V_k\left(x_p\right) =$$

$$\begin{bmatrix} x_{p,k}^T \\ x_{p,k-\varepsilon_k}^T \\ x_{p,k-1}^T \\ \vdots \\ x_{p,k-\varepsilon_M}^T \end{bmatrix}^T \begin{bmatrix} A_p^T P_5 A_p - P_5 + \varepsilon_{M1} P_6 & A_p^T P_5 B_p K_{p,1} & \mathbf{0} & \cdots & \mathbf{0} \\ * & K_{p,1}^T B_p^T P_5 B_p K_{p,1} - P_6 & \mathbf{0} & \cdots & \mathbf{0} \\ * & * & -P_6 & \cdots & \mathbf{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & * & \cdots & -P_6 \end{bmatrix} \begin{bmatrix} x_{p,k} \\ x_{p,k-\varepsilon_k} \\ x_{p,k-1} \\ \vdots \\ x_{p,k-\varepsilon_M} \end{bmatrix} < 0 \tag{73}$$

Now we consider the closed-loop system with disturbances. Substituting the system dynamics (71) into (72) yields

$$V_{k+1}\left(x_p\right) - V_k\left(x_p\right) + \left(G_p x_{p,k}\right)^T \left(G_p x_k\right) - \gamma_2 d_{p,k}^T d_{p,k} = x_{pa,k}^T \Xi_{p1} x_{pa,k} \tag{74}$$

where $x_{pa,k} = \begin{bmatrix} x_{p,k} & x_{p,k-\varepsilon_k} & d_{p,k} & x_{p,k-1} & \cdots & x_{p,k-\varepsilon_{M1}} \end{bmatrix}$ is the augmented states vector and

$$\Xi_{p1} = \begin{bmatrix} A_p^T P_5 A_p - P_5 + \varepsilon_{M1} P_6 + G_p^T G_p & A_p^T P_5 B_p K_{p,1} & A_p^T P_5 D_p & \mathbf{0} & \cdots & \mathbf{0} \\ * & K_{p,1}^T B_p^T P_5 B_p K_{p,1} - P_6 & K_p^T B_p^T P_5 D_p & \mathbf{0} & \cdots & \mathbf{0} \\ * & * & D_p^T P_5 D_p - \gamma_2^2 I & \mathbf{0} & \cdots & \mathbf{0} \\ * & * & * & -P_6 & \cdots & \mathbf{0} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & * & \mathbf{0} & \cdots & -P_6 \end{bmatrix} \tag{75}$$

It is clear that $\Xi_{p1} < 0$ implies that inequality (73) holds thus the system is stable. Moreover, by Lemma 3, $\Xi_{p1} < 0$ is equivalent to $\Xi_{p2} < 0$ where

$$\Xi_{p2} \triangleq \begin{bmatrix} A_p^T P_5 A_p - P_5 + \varepsilon_{M1} P_6 + G_p^T G_p & A_p^T P_5 B_p K_{p,1} & A_p^T P_5 D_p \\ * & K_{p,1}^T B_p^T P_5 B_p K_{p,1} - P_6 & K_p^T B_p^T P_5 D_p \\ * & * & D_p^T P_5 D_p - \gamma_2^2 I \end{bmatrix} \tag{76}$$

Furthermore, Ξ_{p2} can be written as

$$\Xi_{p2} = \begin{bmatrix} -P_5 + \varepsilon_{M1} P_6 & \mathbf{0} & \mathbf{0} \\ * & -P_6 & \mathbf{0} \\ * & * & -\gamma_2^2 I \end{bmatrix} + \begin{bmatrix} P_5 A_p & P_5 B_p K_{p,1} & P_5 D_p \\ G_p & \mathbf{0} & \mathbf{0} \end{bmatrix}^T \begin{bmatrix} P_5^{-1} & \\ & I \end{bmatrix} \begin{bmatrix} P_5 A_p & P_5 B_p K_{p,1} & P_5 D_p \\ G_p & \mathbf{0} & \mathbf{0} \end{bmatrix} \tag{77}$$

With the definition of $M_3 \triangleq P_5 B_p K_{p,1}$, we can conclude $\Xi_{p2} < 0$ (thus $\Xi_{p1} < 0$) from inequality (69) by applying Lemma 3 once again. Next, summing up (74) from 0 to ∞ with respect to k and considering that the system is stable when $\Xi_{p1} < 0$, we have $\sum_{k=0}^{\infty} \left\| G_p x_{p,k} \right\|^2 < \gamma_2^2 \sum_{k=0}^{\infty} \left\| d_{p,k} \right\|^2$. From (77) it can be seen that $\Xi_{p2} < 0$ may not hold if $\varepsilon_{p,k} > \varepsilon_{M1}$ thus the stability of the system cannot be guaranteed.

In Lemma 5, we have shown that the physical system will become unstable once the network delay and packet losses exceed ε_{M1}. In the next theorem, we will show that when the network is experiencing higher delays and packet losses due to network attacks such that $\varepsilon_{p,k} > \varepsilon_{M1}$, the controller gain has to be adjusted in order to maintain stability of the physical system.

Theorem 5: Let $\varepsilon_{p,k}$ be the networked induced overall delay and packet loss as defined by (44). For the case of $\varepsilon_{p,k} > \varepsilon_{M1}$ due to the presence of network attacks, the physical system (71) is stable and satisfies the H_∞ performance constraint if $\varepsilon_{M2} > \varepsilon_{M1}$, where ε_{M2} is maximized value of the following convex optimization LMI problem

$$\begin{aligned} &\text{maximize} && \varepsilon_M \\ &\text{subject to} && P_5 > 0,\ P_6 > 0, \text{ and (45)} \end{aligned} \tag{78}$$

Moreover, the controller gain $K_{p,2}$ for the case of $\varepsilon_{M1} < \varepsilon_{p,k} < \varepsilon_{M2}$ is given by solving

$$P_5 B_p K_{p,2} = M_3 . \tag{79}$$

where M_3, P_5 and P_6 are matrices satisfying (78). However, the stability of the system cannot be guaranteed regardless of the selection of the controller gains if $\varepsilon_{p,k} > \varepsilon_{M2}$.

Proof: By solving the optimization LMI problem (78), we get ε_{M2}, which is the maximum allowed network delay and packet losses that the physical system can tolerate. If $\varepsilon_{M2} \le \varepsilon_{M1}$ then the stability cannot be guaranteed as previously explained. On the other hand, when $\varepsilon_{M2} > \varepsilon_{M1}$, the controller gain is derived by solving (69) with $\varepsilon_M = \varepsilon_{M2}$. The proof of the stability and H_∞ performance in this case is similar to that in the proof of Lemma 5. Likewise, for $\varepsilon_{p,k} > \varepsilon_{M2}$, the stability cannot be guaranteed because $\Xi_{p2} < 0$ in (77) may not hold. Since ε_{M2} is already the maximum allowed value, no controller gain L_p could exist to guarantee (78) for $\varepsilon_{p,k} > \varepsilon_{M2}$.

It is important to note that Theorem 5 gives the maximum network delay and packet losses that the physical system can tolerate. Appropriate network defense must be launched once $\varepsilon_{p,k}$ exceeds this threshold, or the physical system needs to be shut down to prevent further damages.

Therefore, by combining Theorems 4 and 5, the stability of the physical system when the network is under attacks can be predicted. To be specific, Theorem 4 gives the estimated current buffer length $\hat{\rho}_k$ as well as the transmitting rate $\hat{\upsilon}_k$. Thus the current sensor-to-controller delay can be estimated by

$$\hat{\tau}_{sc} = \hat{\rho}_k / \hat{\upsilon}_k . \tag{80}$$

The controller-to-actuator delay $\hat{\tau}_{ca}$ can be estimated in the same way. Furthermore, it is also given in Theorem 4 that the dropped packets by the attack can be estimated by $\hat{\omega}_k$. Therefore, the overall delays and packet losses can be estimated by

$$\hat{\varepsilon} = \hat{\tau}_{sc} + \hat{\tau}_{ca} + \hat{\omega}_k . \tag{81}$$

Next, detection observer is proposed for the physical system in order to detect and isolate attacks on both networks and physical systems. Define the observer as

$$\begin{aligned}\hat{x}_{p,k+1} &= A_p\hat{x}_{p,k} + B_p u_{p,k} + L_p\left(y_{p,k} - \hat{y}_{p,k}\right)\\ \hat{y}_{p,k} &= C_p\hat{x}_{p,k-\varepsilon'}\end{aligned}, \tag{82}$$

Suppose the delay and packet losses increase from ε' to $\varepsilon'+\bar{\varepsilon}$ when the network is experiencing a higher delay and packet losses due to the network attacks. Define the estimation error or physical system detection residual as $\tilde{x}_{p,k} = x_{p,k} - \hat{x}_{p,k}$, then by combining (67) and (82) we have the following estimation error dynamics

$$\tilde{x}_{p,k+1} = A_p\tilde{x}_{p,k} + L_pC_p\tilde{x}_{p,k-\varepsilon'} + L_pC_p\left(x_{p,k-\varepsilon'} - x_{p,k-\varepsilon'-\bar{\varepsilon}}\right) + D_p d_{p,k} + W_p\omega_{p,k}. \tag{83}$$

Let the augmented estimation error vector be

$$\tilde{x}_{pa,k} \triangleq \begin{bmatrix}\tilde{x}_{p,k}^T & \tilde{x}_{p,k-1}^T & \cdots & \tilde{x}_{p,k-\varepsilon'}^T\end{bmatrix}^T \tag{84}$$

Then (83) can be rewritten as

$$\tilde{x}_{pa,k+1} = \tilde{A}_{pa}\tilde{x}_{pa,k} + H_{pa}\left(x_{p,k-\varepsilon'} - x_{p,k-\varepsilon'-\bar{\varepsilon}}\right) + D_{pa}d_{p,k} + W_{pa}\omega_{p,k}\ , \tag{85}$$

where $$\tilde{A}_{pa} = \begin{bmatrix} A_p & \mathbf{0} & \cdots & -L_pC_p \\ I & \cdots & \mathbf{0} & \mathbf{0} \\ \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \cdots & I & \mathbf{0}\end{bmatrix}, \tag{86}$$

and $H_{pa}^T = \begin{bmatrix}L_pC_p & \mathbf{0} & \cdots & \mathbf{0}\end{bmatrix}$, $D_{pa}^T = \begin{bmatrix}D_p & \mathbf{0} & \cdots & \mathbf{0}\end{bmatrix}$, and $W_{pa}^T = \begin{bmatrix}W_p & \mathbf{0} & \cdots & \mathbf{0}\end{bmatrix}$. Next the following lemma is stated to describe the performance of the observer in the absence of attacks.

Lemma 6: Consider the closed-loop physical system (71) and the observer (85) with the disturbance bound $d_{p,M}$ and without any attack i.e. $\omega_{p,k} = 0$ and $\bar{\varepsilon} = 0$. Select the observer

gain matrix L such that the observer representation matrix (86) is stable. Then the estimation error $\tilde{x}_{p,k}$ is bounded by $\Upsilon_{p,k}$ where

$$\Upsilon_{p,k} = \sum_{i=0}^{k-1} \left\| \tilde{A}_{pa}^{k-i-1} \right\| \left\| D_p d_{p,M} \right\| . \tag{87}$$

Proof: The solution of the differential equation (85) is $\tilde{x}_{pa,k} = \sum_{i=0}^{k-1} \tilde{A}_{pa}^{k-i-1} D_p d_{p,k}$. Therefore it follows that

$$\left\| \tilde{x}_{p,k} \right\| \le \left\| \tilde{x}_{pa,k} \right\| \le \sum_{i=0}^{k-1} \left\| \tilde{A}_{pa}^{k-i-1} \right\| \left\| D_p d_{p,M} \right\| . \tag{88}$$

Theorem 6: Consider the closed-loop physical system (71) and the observer (85) with the disturbance bound $d_{p,M}$. Attacks on the physical system or on the communication networks can be detected if $\omega_{p,k}$ and $\bar{\varepsilon}$ satisfies

$$\sum_{i=0}^{k-1} \left\| \tilde{A}_{pa}^{k-i-1} \left(W_{pa} \omega_p + H_{pa} \left(x_{p,k-\varepsilon'} - x_{p,k-\varepsilon'-\bar{\varepsilon}} \right) \right) \right\| > 2\Upsilon_{p,k} . \tag{89}$$

Proof: The proof is similar to that of Theorem 3. If (89) holds, we have

$$\begin{aligned} \left\| \tilde{x}_{pa,k} \right\| &= \left\| \sum_{i=0}^{k-1} \tilde{A}_{pa}^{k-i-1} \left(D_p d_{p,k} + W_{pa} \omega_p + H_{pa} \left(x_{p,k-\varepsilon'} - x_{p,k-\varepsilon'-\bar{\varepsilon}} \right) \right) \right\| \\ &\ge \left\| \sum_{i=0}^{k-1} \tilde{A}_{pa}^{k-i-1} \left(W_{pa} \omega_p + H_{pa} \left(x_{p,k-\varepsilon'} - x_{p,k-\varepsilon'-\bar{\varepsilon}} \right) \right) \right\| - \left\| \sum_{i=0}^{k-1} \tilde{A}_{pa}^{k-i-1} D_p d_{p,k} \right\| > 2\Upsilon_{p,k} - \left\| \sum_{i=0}^{k-1} \tilde{A}_{pa}^{k-i-1} D_p d_{p,k} \right\| > \Upsilon_{p,k} \end{aligned} . \tag{90}$$

It is important to note that this theorem shows the detection scheme on the physical system is able to detect the attacks on the networks due to an increase in the delay and packet losses. However, detecting the attack by the flow observer will be faster when compared to on the physical system. Moreover, the location of the attacks can be determined by applying Theorems 3 and 6 together.

6. SIMULATION AND HARDWARE IMPLEMENTATION RESULTS

In order to show the effectiveness of the proposed attack detection scheme, several scenarios involving both the networks and physical systems are considered in the simulation. On the network side, the first scenario is the simulation for the healthy case where there is no attack. In the next three scenarios, we show the detection results for the attacks introduced in the previous section. In the last scenario, we consider a contrived attack in order to show the limitation of the proposed attack detection scheme.

On the side of the physical plant, we show that the system becomes unstable when the delays and packet losses exceed a certain threshold. Then it is shown that this abnormality in the network flow can be detected by the proposed detection scheme and by reconfiguring the controller gain, the system can be stabilized again. Finally we demonstrate that the proposed detection scheme is able to detect not only the abnormalities in the network, but also attacks on the physical system.

Furthermore, the proposed attack detection for the networks has been implemented in hardware for a wireless sensor network where the results show that both the jamming attack and the blackhole attack can be detected.

6.1. NETWORK SIMULATION RESULTS

The simulation is performed in MATLAB with the following parameters for the communication networks: sampling period $T = 1\text{ms}$, total simulation time $T_s = 200T$, standard transmission rate $\upsilon_0 = 300$ packets per T ,the desired flow in the bottleneck node $\rho_0 = 100$ packets, $m = 3$, $l_1 = 1/8$, $l_1 = 1/4$, $l_1 = 1/2$, the expectation of the delayed measurement $\bar{\alpha} = 0.1$,the bound for the disturbance $d_M = 10$.

6.1.1. Scenario A1 (Normal Case). Let $\omega = 0$ and by solving the LMI (45), we get the following controller and observer gain matrices

$$K = [-0.9971 \quad -2.0174 \quad 0 \quad 0 \quad 0] \text{ and } \quad L = \begin{bmatrix} 0.0191 & 0.9599 & -0.9900 & 0.0564 & 1.0995 \\ 0 & 0.6832 & 0 & 0 & 0 \\ 0.0011 & 0.0024 & 0.3334 & 0.3204 & 0.3250 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0.6813 & 0 \end{bmatrix}.$$

The simulation results for the normal case is plotted in Figure 6.1 and Figure 6.2.

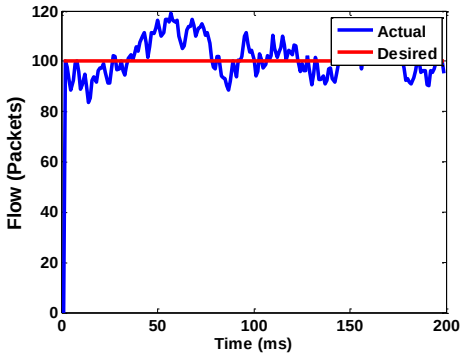


Figure 6.1. Actual flow.

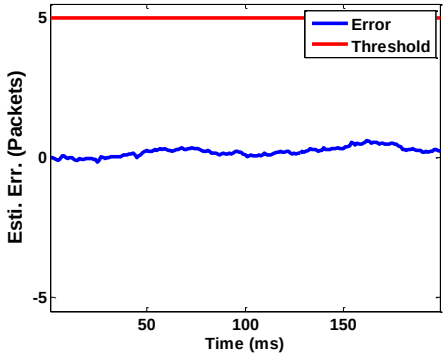


Figure 6.2. Estimation error.

Figure 6.1 shows that the actual flow in the bottle bottleneck node fluctuating slightly around the desired level. Moreover, the estimation error of the flow in the link plotted in Figure 6.2 is very close to zero, concluding that the estimated state given by the observer is fairly accurate. Figure 6.3 shows the input rate while Figure 6.4 shows the output rate at the bottleneck node.

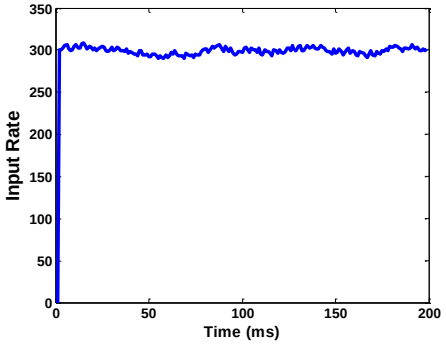


Figure 6.3. Input rate at the bottleneck node.

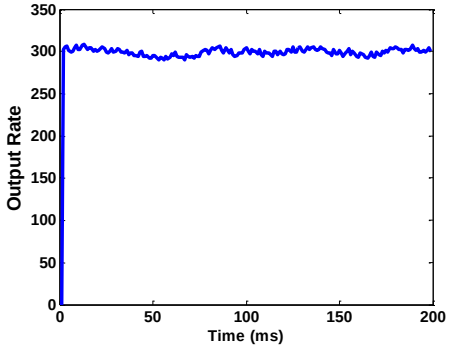


Figure 6.4. Output rate.

6.1.2. Scenario A2~A4. In the following three scenarios, jamming attack, blackhole attack, and minimum rate DoS stream attack has been launch at $T_s/2$, respectively. In Scenario A2, the attacker is assumed to increase the number of jammers in the network linearly along with the time until to the maximum value. As a result, the packets injected by the attacker increase until to the maximum of 5 packets per millisecond, as plotted in Figure .6.5. The estimation error of the flow, plotted in Figure 6.6, exceeds the threshold shortly after the attack is launched and thus it can be detected.

Upon detection, if the new observer introduced in Theorem 4 is applied, then the attack flow can be estimated as shown in Figure 6.5. Correspondingly, the attack residual with the new observer decreases after the detection of the attack and eventually becomes smaller than the threshold. With the estimated attack flow, one can estimate the delay and packet losses in the link, which can be further utilized to tune the controller parameters of the physical systems.

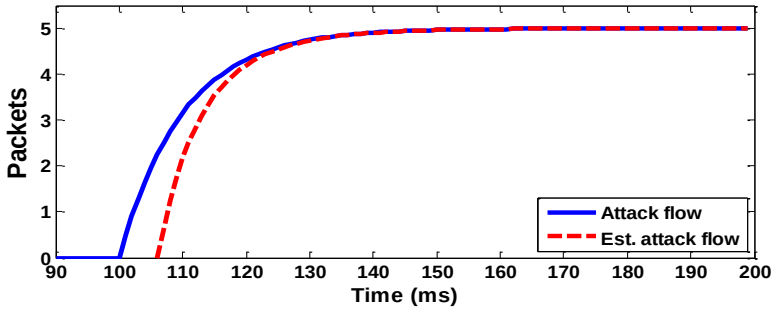


Figure 6.5. Injected flow by the jamming attack with estimation.

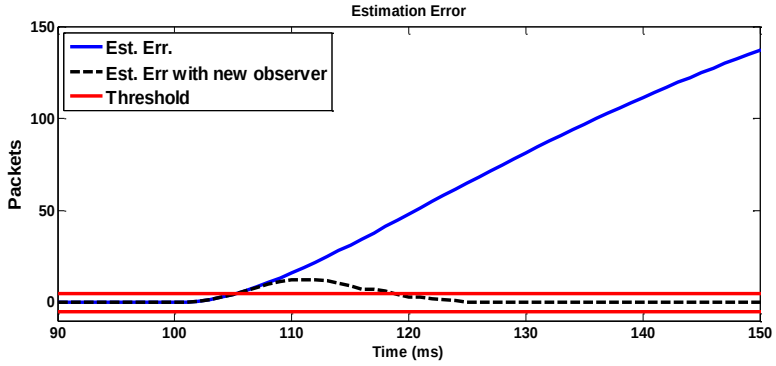


Figure 6.6. Estimation error in Scenario A2.

Similarly, in Scenario A3, we assume the nodes compromised by the black hole attack increases linearly as displayed in Figure 6.7. Consequently, the estimation error exceeds the lower bound of the threshold and the attack can be detected after 10 sampling periods, as shown in Figure 6.8.

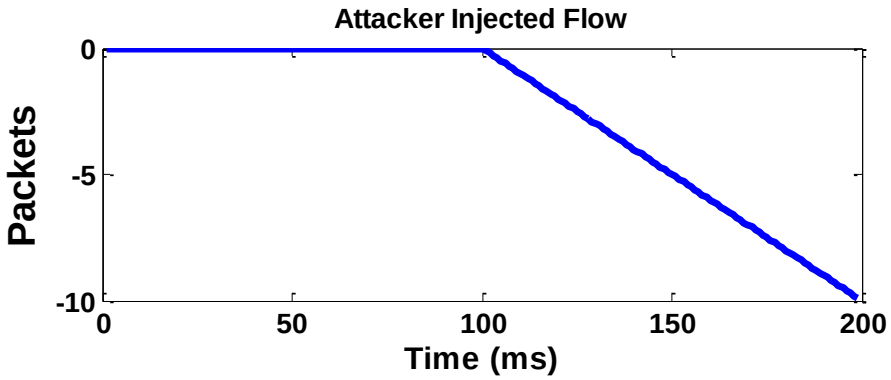


Figure 6.7. Dropped flow by the black hole attacker.

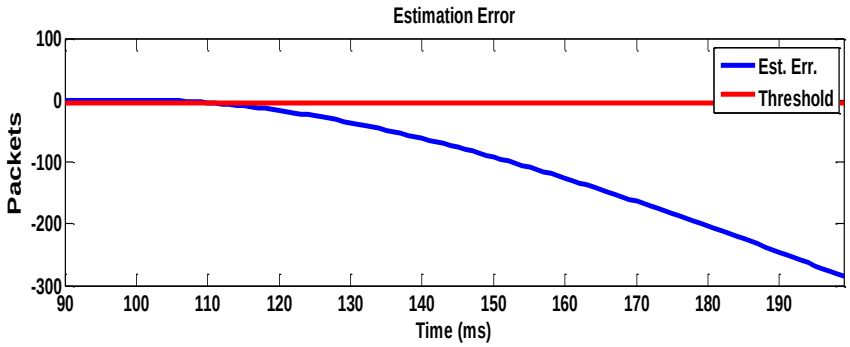


Figure 6.8. Estimation error in Scenario A3.

In Scenario A4, we launch the minimum rate DoS stream attack as shown in Figure 6.9 with the following parameters $n_1 = 5$, $n_2 = 1$, $p_1 = 2T$, $p_1 = 5T$ and $\tilde{T} = 20T$. As shown in Figure 6.10, although the estimation error increases slower than those in Scenario A2 and A3, the attack can still be detected as due to the high-data-injecting-rate period of the attack.

6.1.3. Scenario A5. In this scenario we consider a type of attack with a special pattern. We let the attack drop a few packets first and followed by injecting the same amount of packets, as plotted in Figure 6.11.

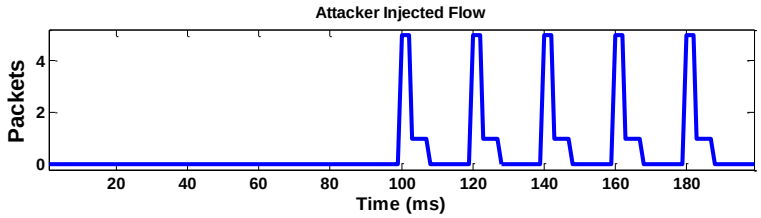


Figure 6.9. Injected flow by the Minimum rate DoS attacker.

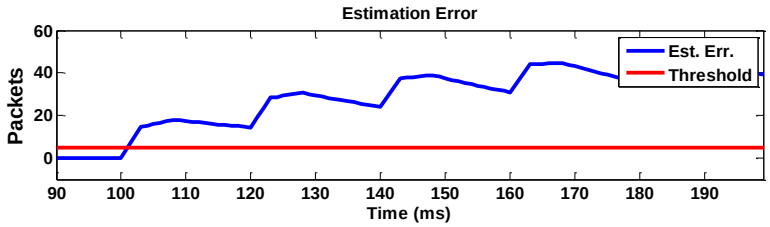


Figure 6.10. Estimation error in Scenario A4.

Note that the number of packets that are injected (dropped) is identical with that during high-data-injecting-rate period of the Minimum rate DoS stream attack in Scenario A4. However, as plotted in Figure 6.12, the estimation error never exceeds the threshold

due to the fact that it is updated in an accumulated way. Due to the delayed measurement feeding into the observer, the current positive estimation is counteracted with the previous negative ones, resulting in an insignificant change in the estimation error compared with the actual variation of the packets in the link. Therefore, this type of attack cannot be detected by the proposed detection scheme.

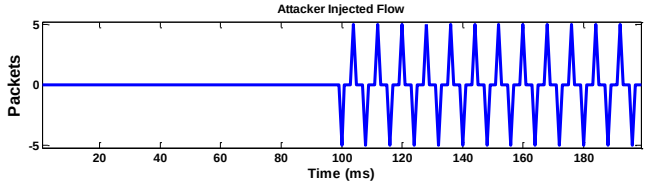


Figure 6.11. Injected and dropped flow in Scenario.

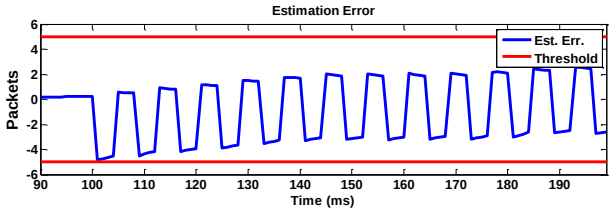


Figure 6.12. Estimation error in Scenario A5.

6.2. SIMULATION RESULTS FOR THE PHYSICAL SYSTEMS

The network attack is launched at T=10s and increases its attacking strength at T=20s. (a): regulation errors when the same controller gain is applied through the simulation; (b): the estimation error; (c): regulation errors when the controller gain is re-configured at T=10s, as shown in Figure 6.13

The batch reactor system, which is a benchmark example for studying NCS [30], is considered in the simulation of the physical system. The continuous system dynamics are given by

$$\dot{x} = \begin{bmatrix} 1.38 & -0.2077 & 6.715 & -5.676 \\ -0.5814 & -4.29 & 0 & 0.675 \\ 1.067 & 4.273 & -6.654 & 5.893 \\ 0.048 & 4.273 & 1.343 & -2.104 \end{bmatrix} x + \begin{bmatrix} 0 & 0 \\ 5.679 & 0 \\ 1.136 & -3.146 \\ 1.136 & 0 \end{bmatrix} u$$
$$y = \begin{bmatrix} 0 & 0.3 & 0.3 & 0 \\ 0.6 & 0.3 & 0.6 & 0.3 \end{bmatrix} x \qquad (91)$$

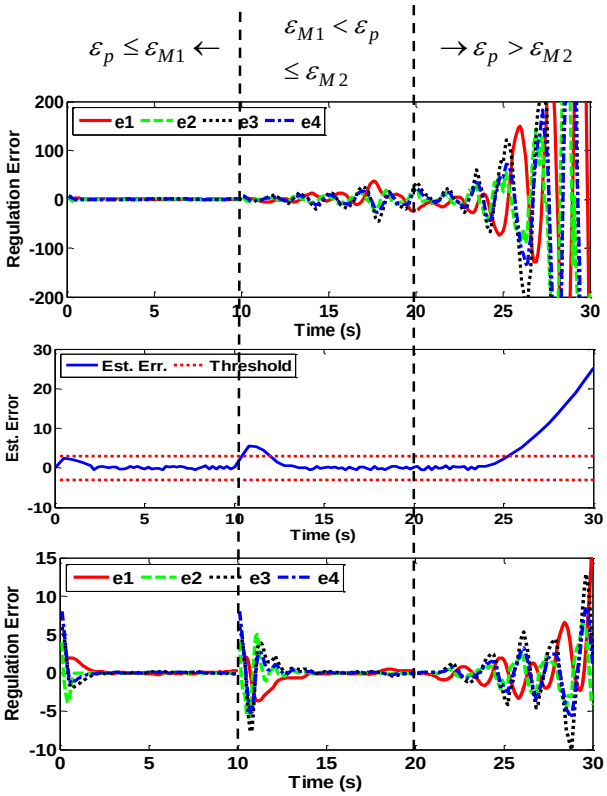
The system is discretized with the sampling period $T_{p,s} = 100ms$. The disturbance $\omega_{p,k}$ follows the uniform distribution within the interval $[-0.5, 0.5]$. The total simulation time is 30 seconds.

1) $T = 0 - 10s$ ($\varepsilon_p \le \varepsilon_{M1}$). For the first 10 seconds, we consider the healthy case where there are no attacks either on the network or on the physical system. As a result, the delays and packet losses are bounded by $\varepsilon_{M1} = 2$. Solving the LMI (69) with $\gamma_2 = 5$ yields the controller gain

$$K_{p,1} = [0.49, 0.21, -0.47, -0.38; 1.79, 0.27, 2.30, 0.77].$$

The simulation results are shown in Figure 6.13 (a) where the regulation error is fairly close to zero and thus the system is stable with $K = K_{p,1}$.

2) $T = 10 - 20s$ ($\varepsilon_{M1} < \varepsilon_p \le \varepsilon_{M2}$). Next, we launch the jamming attack introduced in Scenario A2 on the communication networks at $T = 10s$.



(a)

(b)

(c)

Figure 6.13. Simulation results for the attack detection on the physical system.

By adjusting the attack strength, we set the delays and packet losses satisfying $3 \le \varepsilon_p \le 4$, which has exceeded the threshold $\varepsilon_{M1} = 2$. Figure 6.13 (a) shows the simulation results if the same controller gain $K_{p,1}$ is applied. It is clear that the regulation errors do not converge, because the delays and packet losses exceed the threshold and inequality (73) cannot be satisfied. These results agree with the conclusion from Lemma 5.

However, consider that the physical system is implemented with the observer-based attack detection scheme (82). Then as shown in Figure 6.13 (b), the estimation error quickly exceeds the threshold thus the attack can be detected. Since it is shown in Scenario B2 that

the controller gain $K_{p,1}$ cannot stabilize the system in this case, we need to compute the controller gain by solving the optimization LMI problem (78). As a result, we obtain $\varepsilon_{M2} = 5.8$ and $K_{p,2} = [-0.42, -0.52, -0.43, -0.27; 1.62, 0.20, 1.14, -0.64]$.

Figure 6.13 (c) shows the convergence of the regulation errors when the new controller gain $K_{p,2}$ is applied. Combining Scenario B2 and B3, we can come to the conclusion that the attacks on the networks can be detected and upon the detection, the physical plant can be stabilized by selecting the appropriate controller gain.

3) $T = 20 - 30s$ ($\varepsilon_p > \varepsilon_{M2}$). Suppose that the attacker increases the attack strength at the time $T = 20s$ such that $\varepsilon_p > \varepsilon_{M2}$. As shown in Figure 6.13 (a), the system becomes unstable even if the new controller gain $K_{p,2}$ is applied, which verifies the conclusion in Theorem 5.

6.3. PHYSICAL SYSTEM ATTACK DETECTION

It is shown in the previous simulation results that the proposed attack detection scheme is capable of detecting attacks on the network that leads to an increase in the delays and packet losses. Next, it is of interest to study the detectability launched on the physical system directly either through sensor, actuator or other means. Consider an attack launched at $T = 5s$ with $\omega_{p,k} = -0.2e^{0.1k}$.

As shown in Figure 6.14, the state estimation error increases and exceeds the threshold shortly after the attack has been launched at the physical system. Therefore, the attack can be detected, which verifies the correctness of Theorem 6.

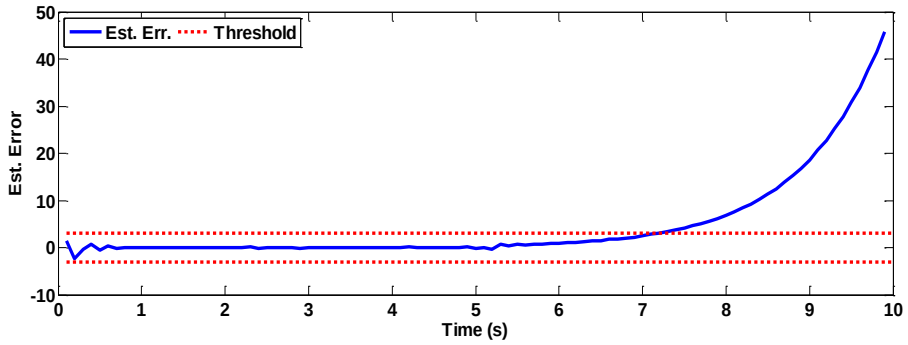


Figure 6.14. Detection of attacks on the physical systems.

6.4. HARDWARE IMPLEMENTATION

The proposed flow based network attack detection scheme is implemented in a wireless sensor network where the RIFD reader collects the data from the RFID sensors then sends to the server through a ZigBee network. As shown in Figure 6.15, the links between the RFID reader and the XBee modules as well as the ZigBee networks are vulnerable to malicious attacks.

Two types of attacks are considered here: 1) the jamming attack where the attacker places a transmitter in order to create congestion in the ZigBee network; 2) the blackhole attack where the attacker blocks the signal of the input node, which causes data losses in the link.

The proposed flow based attack detection scheme has been implemented on the source node and for the purpose of demonstration, all the data including the estimation errors will be sent to the server where a simple user interface has been developed. As shown in Figure 6.16 (a), the red lines are the lower and higher detection thresholds while the blue

line is the flow estimation error, which is the difference between the expected and the actual flow. The estimation error should stay within the bound if there are no attacks launched, as verified in Figure 6.8.

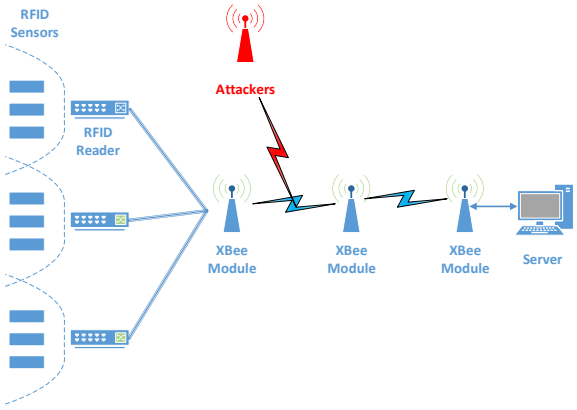
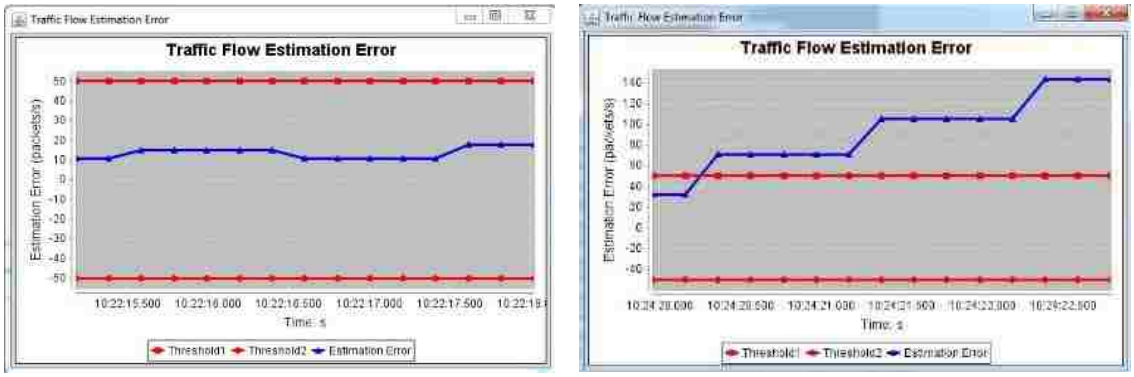


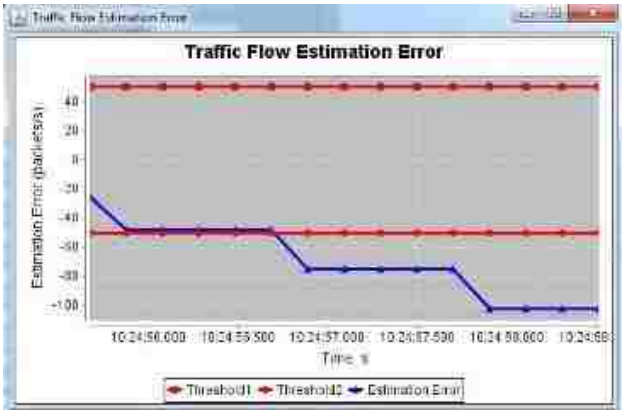
Figure 6.15. Diagram of the hardware implementation.

Next, we launch the jamming attack by placing a transmitter which constantly sends data to the ZigBee network. As a result, more flow is introduced and the attack can be detected when the estimation error of the traffic flow exceeds the upper threshold, as verified in Figure 6.16 (b). Similarly, we launch the blackhole attack by blocking the signal of the input node for some certain time. The attack can be detected when the estimation error of the traffic flow exceeds the lower threshold, as verified in Figure 6.16 (c). Though

this hardware implementation does not include the physical system, the effect of the network within the feedback loop is shown through simulation.



(a) (b)



(c)

Figure 6.16. Estimation error for (a) the normal scenario; (b) the jamming attack scenario; (c) the blackhole attack scenario.

7. CONCLUSIONS AND FUTURE WORK

The presence of communication links to transmit sensor data and control commands has brought in vulnerabilities into NCS. A corrupted communication link can introduce large delays and packet losses, which could lead to the instability of the physical system. This paper proposes a novel cyber-attack detection scheme that is capable of capturing the abnormality in those communication links. The detection of the attacks is faster than the traditional approach where one has to wait for the physical states to be deteriorated. With the proposed detection scheme, attacks on both the networks and the physical system can be detected. Upon detection, the physical system can be stabilized by re-configuring the controller gain. However, the proposed scheme is applicable only to those network attacks causing delays and packets losses while revealing limitation to sophisticated attacks as discussed in Section VI. Dealing with sophisticated attacks remains part of the future work.

8. REFERENCES

[1] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," Automatica, vol. 51, pp. 135-148, 2015.

[2] H. Sandberg, S. Amin, and K. H. Johansson, "Cyber-physical security in networked control systems: an introduction to the issue," IEEE Control Systems, vol. 35, no. 1, pp. 20-23, 2015.

[3] H. Baumman and W. Sandmann, "Markovian modeling and security measure analysis for networks under flooding DoS attacks," 20th Euromicro International Conferences on the Parallel, Distributed and Network-based Processing, pp. 298-302, March 2012.

[4] Q. Zhu and T. Basar, "Robust and resilient control design for cyber-physical systems with an application to power systems," 50th IEEE Conference on Decision and Control and European Control Conference, pp. 4066-4071, December 2011.

[5] C.W. Ten, G. Manimaran, and C.C. Liu, "Cybersecurity for critical infrastructures: attack and defense modeling," IEEE Transactions on Systems, Management, and Cybernetics, vol. 40, no. 4, pp. 853-865, July 2010.

[6] K. Sallhammar, B.E. Helvik, and S.J. Knapskog, "Towards a stochastic model for integrated security and dependability evaluation," IEEE Conference on Availability, reliability and Security, pp. 1-8, September 2006.

[7] A. Aenes, K. Salhammar, K. Haslum, T. Brekne, M. Moe, and S. J. Knapskog, "Realtime risk assessment with network sensors and intrusion detection systems," International Conference on Computational Intellengence and Security, pp. 388-397, December 2005.

[8] C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," American Control Conference (ACC), pp. 3344-3349, June 2013.

[9] L. Liu, M., Esmalifalak, Q. Ding, V. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," IEEE Transaction on Smart Grid, vol. 5, no. 2, pp. 612-621, 2014.

[10] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. Sastry, "Cyber security analysis of state estimators in electric power systems," IEEE Conference on Decision Control, pp. 5991-5998, December 2010.

[11] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," IEEE Transactions on Automatic Control, vol. 59, no. 6, pp. 1454-1467, 2014.

[12] S. Amin, A. Cárdenas, and S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," Hybrid System Computer Control, vol. 5469, pp. 31–45, April 2009.

[13] M. Zhu and S. Martínez, "Stackelberg game analysis of correlated attacks in cyber-physical systems," American Control Conference, pp. 4063-4068, July 2011.

[14] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," IEEE Transaction on Automatic Control, vol. 58, no. 11, pp. 2715-2729, 2013.

[15] H. Niu and S. Jagannathan, "Optimal defense and control of dynamic systems modeled as cyber-physical systems," Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, vol. 12, no. 4, pp. 423-438, 2015.

[16] H. Xu, S. Jagannathan, and F. L. Lewis, "Stochastic optimal control of unknown linear networked control system in the presence of random delays and packet losses," Automatica vol. 48, no. 6, pp. 1017-1030, 2012.

[17] J. C. Bolot, "End-to-end packet delay and loss behavior in the Internet," In ACM SIGCOMM Computer Communication Review, vol. 23, no. 4, pp. 289-298, 1993.

[18] Y. T. Hou, S. S. Panwar, and H. Tzeng, "On generalized max-min rate allocation and distributed convergence algorithm for packet networks," Parallel and Distributed Systems, IEEE Transactions on 15, no. 5, pp. 401-416, 2014.

[19] E. Altman, and T. Basar, "Optimal rate control for high speed telecommunication networks," In Decision and Control, Proceedings of the 34th IEEE Conference on, vol. 2, pp. 1389-1394, December 1995.

[20] S. Keshav, "A control-theoretic approach to flow control," ACM, vol. 21, no. 4, pp. 3-15, 1991.

[21] F. Yang, Z. Wang, Y. S. Hung, and M. Gani, "H-infinity control for networked systems with random communication delays," Automatic Control, IEEE Transactions on, no. 3, pp. 511-518, 2006.

[22] E. Bouhtouri, D. H. Abdelmoulah, and A. J. Pritchard, "H-infinity type control for discrete-time stochastic systems," Inst. fur Dynamische Systeme, Fachbereich Mathematik und Informatik, vol. 36, no. 5, pp. 1504-1538. 1998.

[23] T. J. Tarn, and Y. Rasis, "Observers for nonlinear stochastic systems," Automatic Control, IEEE Transactions on, vol. 21, no. 4, pp. 441-448, 1976.

[24] R. A. Horn and C.R. Johnson, "Topics in matrix analysis," Cambridge University Press, New York, 1991.

[25] X. Luan, S. Peng, and F. Liu, "Stabilization of networked control systems with random delays," Industrial Electronics, IEEE Transactions on 58, no. 9, pp. 4323-4330, 2011.

[26] M. Bishop, Computer Security: Art and Science, vol. 200. Addison-Wesley, 2012.

[27] P. Tague, D. Slater, R. Poovendran, and G. Noubir, "Linear programming models for jamming attacks on network traffic flows," In Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops, IEEE 6th International Symposium on, pp. 207-216, May 2008.

[28] P. Raj, and P. B. Swadas, "Dpraodv: A dyanamic learning system against blackhole attack in AODV based MANET," arXiv preprint: 0909.2371, 2009.

[29] A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants," In Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communications, pp. 75-86. ACM, August 2003.

[30] D. Carnevale, A. Teel, and D. Nesic, "A Lyapnov proof of improved maximum allowable transfer interval for networked control systems," IEEE Transactions on Automatic Control, vol. 52, pp. 892–897, 2007.

IV. AN OPTIMAL Q-LEARNING APPROACH FOR ATTACK DETECTION IN NETWORKED CONTROL SYSTEMS

Haifeng Niu and S. Jagannathan

In networked control systems, both the communication links and the physical systems are vulnerable to a variety of attacks. Attacks on the networks may falsify sensitive data, cause link congestion and/or increase the number of lost packets. As a consequence, the physical system whose feedback loop relies on these infected networks then becomes uncertain. Moreover, attacks on the physical systems targeting the sensors or the actuators may degrade the performance or even lead to the instability of the overall system. In this paper, we propose a novel attack detection scheme that is capable of detecting attacks on both the network and the physical system. The network traffic flow is modeled as a linear system with unknown system dynamics and an optimal Q-learning based controller is developed to stabilize the flow in the presence of disturbances. An adaptive observer is proposed to generate the attack residual, which is utilized to determine the onset of an attack when it exceeds a predefined threshold. For the physical system, we consider a stochastic system which incorporates network-induced delays and packet losses making the system dynamics uncertain. The proposed detection scheme includes an optimal Q-learning based event-triggered controller which is capable of detecting attacks on both sensors and actuators.

1. INTRODUCTION

Networked control systems (NCS) consists of the system to be controlled, sensors, actuators, and controllers where different components coordinate through a communication network. Although after over thirty years' development NCS are fairly mature with applications in areas varying from large-scale industrial systems to critical infrastructure, there are also challenging problems for current research.

Due to the nature of NCS where its components are spatially distributed, the communication networks between different components can be vulnerable to potential malicious attacks. For example, the wormhole attacker attracts data traffic by establishing a link between two geographically distant regions of the network with high-gain antennas and then delays or drops the attracted data [1]. The jamming attacks over wireless networks, which are inevitable due to the shared nature of wireless channels, may severely degrade the performance in terms of message delay and data throughput by broadcasting radio interferences [2]. The replay attacker maliciously repeats the messages delivered from the operator to the actuator and causes communication unreliability, which has been successfully used by the virus attack of Stuxnet [3][4].

Note that none of the attacks mentioned above requires the knowledge of cryptographic mechanisms. That is to say, the efforts in [5-7] proposing encryption algorithms that are specially designed for the low-cost and resource-restrained devices for NCS cannot protect the network security from those attacks. However, one common attribute shared by these attacks is that they all tend to deviate the amount of traffic flow in the communication links from the normal value though this traffic flow due to these

attacks may not be known beforehand. Inspired by this observation, we propose the traffic flow-based network attack detection scheme.

Flow control has been studied in the literature [8-11]. For example, the authors in [8] model the high-speed network as fluid-flow queues with a fixed propagation delay for each channel. As a result, the network is represented by a linear hybrid system, which allows the design of the flow control on a mathematical basis. In [9], a receiver-based flow control scheme is proposed that achieves the given optimal utility. The proposed flow control scheme creates virtual queues at the receivers as a push-back mechanism to optimize the amount of data delivered to the destinations via back-pressure routing. Different from [9], the authors in [10] propose a new utility max-min flow control framework using classic sliding mode control. The framework consists of a source algorithm and a binary congestion feedback mechanism and is proven to be asymptotically stable by Lyapunov-based theorem. In [11], a new joint flow control and scheduling algorithm for multi-hop wireless networks is proposed. Unlike traditional solutions based on the back-pressure algorithm, the proposed algorithm combines window-based flow control with a new rate-based distributed scheduling algorithm.

However, to the best of our knowledge, minimal effort has been spent on studying the flow control from the perspective of network security when the network is attacked by injecting or dropping traffic flow. Moreover, it is also challenging to regulate the traffic flow at the desired level in the presence of disturbances and attacks, especially when the system dynamics that characterize the network parameters are unknown.

On the other hand, the physical system whose feedback loop relies on the communication networks becomes uncertain in the presence of cyber-attacks. In other

words, a vulnerable communication network results in larger delays and higher packet loss ratios, which could further lead to the instability of the physical system [12]. To address this issue, the authors in [12] incorporate uncertain network-induced delays and packet losses in the physical system dynamics and propose a stochastic adaptive dynamic programming (ADP) approach to estimate the value function and solve the optimal regulation problem. This work is further extended in [13] by adopting the stochastic ADP technique in an event-driven control scheme, which is reported to significantly reduce the computation and data transmission. Furthermore, this event-driven control scheme is improved in [14] by utilizing the interval between the sampling instants for iterative parameter learning updates. This hybrid Q-learning algorithm renders a higher efficiency of the optimal regulator.

However, the physical system is also subject to attacks, which is not considered in the above mentioned effort [12-14]. For instance, an attacker can manipulate the physical behavior of a system by exploiting the vulnerabilities of the sensors and attempting to modify or send falsified sensor data to the controller [15]. Similarly, the attacker may also sabotage the actuator and cause chaos or calamity immediately since the actuator is the final step in the control chain when the control instructions are made physically real [16]. Therefore, it is critical to take the attack input into account and implement an attack detection scheme for the physical system.

Therefore, in this paper, we propose a detection scheme that is capable of capturing the abnormal traffic flow in the networks for certain class of cyber-attacks by modeling the flow as a linear system with unknown dynamics. Likewise, an attack detection scheme is

proposed to detect both sensor and actuator attacks on the physical system, whose dynamics are uncertain due to the networked-induced delays and packet losses.

We begin by introducing the state–space representation of traffic flow in the presence of disturbances and cyber-attacks. Since the network parameters such as the service rate are usually unknown, we consider the system dynamics of the traffic flow as unknown. Next, we derive the optimal controller by using Q-learning technique that stabilizes the flow during healthy conditions. The network attack detection residual is generated which in turn is utilized to determine the onset of an attack in the communication network when the residual exceeds a predefined threshold. Then the detectability condition is introduced and the performance of the attack estimation scheme is discussed.

Next, we introduce an attack detection scheme for the physical system whose dynamics are uncertain due to the network-induced delays and packet losses. The event-triggered optimal control scheme is adopted since it is proven to reduce network traffic which might help to mitigate congestion in the presence of attacks in the event that attacks increase traffic flow. Finally the proposed scheme is evaluated though the simulation. The results verify that the proposed scheme for the networks is able to detect certain types of attacks and the attacks on the physical system can also be detected.

The contributions of the paper include: 1) the design of the optimal flow controller in the presence of disturbances and cyber-attacks, where the network parameters are considered as unknown; 2) the development of novel observer-based network attack detection and estimation scheme along with detectability condition; 3) the development of sensor/actuator attack detection scheme with an event-triggered controller for the physical system with uncertain system dynamics; 4) the derivation of the maximum network-

induced delays and packet losses that the physical system can tolerate; and 5) demonstration of the proposed scheme in both simulation in the presence of a class of attacks with specific adversary models.

The rest of this paper is organized as follows. In Section 2, we introduce the state-space stochastic flow model under cyber-attacks. The observer and controller design is presented in Section 3, followed by the adversary model and cyber-attack detectability provided in Section 4. In Section 5 we present the detection scheme and controller design for the physical system. The simulation as well as the hardware implementation results and analysis are given in Section 6 and conclusions in Section 7.

The notations used in the paper are briefly introduced. $E\{x\}$ denotes the expectation of the stochastic variable x, $\lambda_{\max}\{M\}$ represents the largest eigenvalue of matrix M, $[M]_{ij}$ represents the element in the i^{th} row and j^{th} column of matrix M and I_n denotes the n-dimensional identity matrix.

2. LINEAR FLOW MODEL WITH UNKNOWN DYNAMICS

Figure 2.1 shows the diagram of a typical NCS, in which both the controller commands and the sensor data are transmitted through a wired or wireless communication link. In this section, we propose a stochastic state-space representation in discrete-time for the traffic flow at the bottleneck link in the presence of attacks, where the network parameters are considered as unknown.

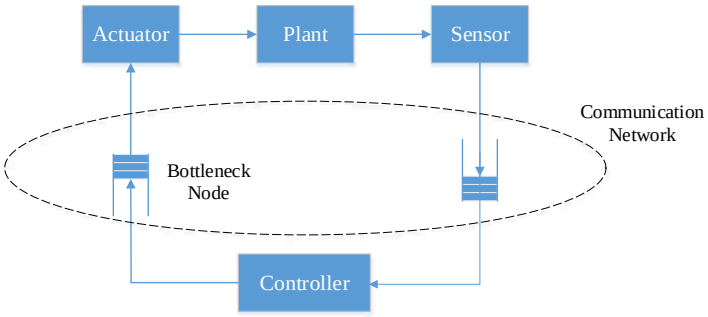


Figure 2.1. Diagram of a typical NCS.

It is verified both theoretically and experimentally [17] that the performance measures such as the delay and transmission rate are determined by the bottleneck node and therefore a mild assumption widely reported in the literature [18][19] is asserte.

Let the input rate at sampling time kT be $\bar{\mu}_k$ packets per second and u_k be the adjustment from the previous input rate, that is

$$\bar{\mu}_k = \bar{\mu}_{k-1} + u_k. \tag{1}$$

The transmission or service rate $\bar{\upsilon}_k$, which slightly fluctuates around the standard transmission rate υ_0, is modeled by a stable autoregressive–moving-average (ARMA) process given by [19]

$$\bar{\upsilon}_k = \upsilon_0 + \delta_k, \tag{2}$$

where

$$\delta_k = \sum_{i=1}^{m} l_i \delta_{k-i} + d_{k-1}, \tag{3}$$

and d_k represents a bounded disturbance with d_M being its bound while the constant m is the number of past values used in ARMA model which can be obtained during system identification and the weights l_i are unknown constants. Compared with other transmission rate models such as the random walk model [19], the advantages with the ARMA process is that it is analytically tractable and capable of capturing a wide range of possible behavior.

Let the traffic flow in the bottleneck node at time kT be $\bar{\rho}_k$. Then we have

$$\bar{\rho}_{k+1} = \bar{\rho}_k + T\bar{\mu}_k - T\bar{\upsilon}_k + \bar{w}_k, \tag{4}$$

where w_k is the number of the packets introduced by the attack flow with $w_k > 0$ implies that the attack has injected data while $w_k < 0$ implies that the attack has dropped data. More detailed representation of the attack models can be found in Section 4. Let the desired flow at the bottleneck node be ρ_0 and re-write (4) as

$$\bar{\rho}_{k+1} - \rho_0 = (\bar{\rho}_k - \rho_0) + T(\bar{\mu}_k - \nu_0) - T\delta_k + w_k . \tag{5}$$

Now define the shifted flow ρ_k and input rate μ_k as

$$\rho_k = \bar{\rho}_k - \rho_0, \mu_k = \bar{\mu}_k - \upsilon_0 . \tag{6}$$

Then the flow dynamic in (4) become

$$\rho_{k+1} = \rho_k + T\mu_k - T\delta_k + w_k . \tag{7}$$

Define the state vector $x_k = \left[\rho_k, \mu_k, \delta_k, \cdots, \delta_{k-m+1}\right]^T$ [19] and assume that the attack input is a function of the state $w_k = w\left(x_k\right)$. Then combining (1), (3) and (7) yields

$$\begin{bmatrix} \rho_{k+1} \\ \mu_{k+1} \\ \delta_{k+1} \\ \delta_k \\ \vdots \\ \delta_{k-m+2} \end{bmatrix} = \begin{bmatrix} 1 & T & -T & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & l_1 & \cdots & l_{m-1} & l_m \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \begin{bmatrix} \rho_k \\ \mu_k \\ \delta_k \\ \delta_{k-1} \\ \vdots \\ \delta_{k-m+1} \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} u_k + \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} d_k + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} w_k . \tag{8}$$

or

$$x_{k+1} = Ax_k + Bu_k + Dd_k + Ww_k , \tag{9}$$

where $A \in \Re^{n \times n}$, B, D, and $W \in \Re^{n \times 1}$ represents the corresponding matrices from (8) with $n \triangleq m+2$. The attack input w_k is unknown but deterministic [1][20][21]. Moreover, the system output is defined as

$$y_k = \begin{bmatrix} \tau_k \\ \chi_k \end{bmatrix} = \begin{bmatrix} f_\tau\left(x_k\right) \\ f_\chi\left(x_k\right) \end{bmatrix} + \begin{bmatrix} v_{\tau,k} \\ v_{\chi,k} \end{bmatrix} , \tag{10}$$

where τ_k is the link end-to-end delay and χ_k is the packet loss rate. The functions f_τ and f_χ are protocol-dependent functions, which can be either deterministic or stochastic [22].

The noise sources $v_{\tau,k}$ and $v_{\chi,k}$ are immeasurable random values following a certain distribution [23].

Assumption 1: The network delays and packet losses are primarily determined by the network protocol and the state x_k including the input rate, buffer length, and the service rate. However, the delays and packet losses become stochastic because they are also affected by many stochastic factors such as the node processing speed, number of hops in the link and also measurement noise [22] [23]. For example, the delay in ARQ-enabled slotted radio networks follows the Poisson distribution with the expected value being

$$E\{\tau\} = \frac{T_F}{2}\left(1 + \frac{\rho T_F\left(1+P_\tau\right)}{\left(1-\pi_\tau\right)\left(1-P_\tau\right)^2}\right)$$

where ρ is the buffer length and other variables are protocol-dependent parameters defined in [24]. The Internet time-delay can be modeled as $\tau_k = \sum_{i=0}^{n}\left(\frac{l_{\tau,i}}{C_\tau} + \frac{\rho}{b_\tau} + t_i^R + v_{L,k}\right)$ where $v_{L,k}$ is the noise and other variables are protocol-dependent parameters defined in [25].

Remark 1: Note that matrix A is unknown because the weights l_1, …, l_m of the ARMA process introduced in (3) are unknown . Therefore, an adaptive observer is utilized in order to estimate the unknown matrix A, which is presented in Section 3.1.

It has been reported in the literature [20] that the network state can be easily measured when the servers at the output queues are Rate Allocating Servers and the transport protocol supports the Packet-Pair probing technique. Therefore, in this paper, the network state in the link is considered accessible. Now we are ready to introduce the flow observer and controller. Note that controller will be utilized for the system (9) in the absence of network attacks first.

3. FLOW OBSERVER AND CONTROLLER DESIGN

In this section, we first introduce the adaptive observer used to estimate the unknown system dynamics. Then we show the convergence of the estimation error for the unknown parameters in the absence of attacks. Next, the Q-learning based optimal network flow controller is introduced along with the stability analysis.

3.1. PARAMETER ESTIMATION

The benefit of the observer is twofold. On one hand, the unknown system dynamics A needs to be estimated in order to compute the appropriate control input. On the other hand, by using the measured and estimated states, an estimation error or attack residual is generated for detection. The observer is described as

$$\hat{x}_{k+1} = \hat{A}_k \hat{x}_k - A_m \left(x_k - \hat{x}_k \right) + B u_k , \tag{11}$$

where $\hat{x}_k \in \Re^{n\times 1}$ and $\hat{A}_k \in \Re^{n\times n}$ is the estimated states and matrix A, respectively. The matrix $A_m \in \Re^{n\times n}$ is a stable matrix satisfying a certain condition to be derived later.

Define the estimation error of the matrix A as $\tilde{A}_k \triangleq A - \hat{A}_k$, and the estimation error of the state vector as $\tilde{x}_k \triangleq x_k - \hat{x}_k$. Then combining (11) and (9) with $w_k = 0$ yields the system state error dynamics, which is given by

$$\tilde{x}_{k+1} = A_s \tilde{x}_k + \tilde{A}_k \hat{x}_k + D d_k , \tag{12}$$

where $A_s \triangleq A - A_m$. The following assumption is needed before we proceed.

Assumption 1: Assume that the attack is launched after the convergence of the parameter estimation. This assumption is reasonable because in the presence of attacks, it is impossible to determine whether the state estimation error is caused by the attack input or

by the identification error. As a result, the state estimating error and the identification error may never converge. Next, we show in the following theorem that with the given update law for the parameter estimation, the estimation error of the matrix A and state vector x are both ultimately bounded (UB).

Theorem 1 (Parameter Estimation): Consider the network traffic represented as a flow at the bottleneck node described by (9). Let the adaptive observer be described by (11) with the following update law

$$\hat{A}_{k+1} = \hat{A}_k + \beta_1 \frac{\hat{x}_k \tilde{x}_{k+1}^T}{\|\hat{x}_k\|^2 + 1}, \tag{13}$$

where $\beta_1 \in \Re^+$ is the design parameter satisfying

$$0 < \beta_1 < \min\left\{ \frac{2\left(1 - 4\|A_s\|^2\right)}{\|A_s\|}, \frac{\|\hat{x}_k\|^2}{\left(1 + \|\hat{x}_k\|^2\right)^2 + 1} \right\}. \tag{14}$$

Then in the presence of bounded disturbances ($|d_k| \le d_M$) and in the absence of network attacks ($w_k = 0$), both the parameter estimation error $\tilde{A}_k$ and the state estimation error $\tilde{x}_k$ are UB.

Proof: According to (13), the error dynamics of the unknown system matrix A is given by

$$\tilde{A}_{k+1} = \tilde{A}_k - \beta_1 \frac{\hat{x}_k \tilde{x}_{k+1}^T}{\|\hat{x}_k\|^2 + 1}. \tag{15}$$

Select the Lyapunov function as

$$L_{o,k} = \tilde{x}_k^T \Lambda_1 \tilde{x}_k + tr\left\{\tilde{A}_k^T \tilde{A}_k\right\}, \tag{16}$$

where $\Lambda_1 \in \Re^{n \times n}$ is a positive definite matrix. Then the first difference of $L_{o,k}$ is given by

$$\Delta L_{o,k} = \tilde{x}_{k+1}^T \Lambda_1 \tilde{x}_{k+1} + tr\left\{\tilde{A}_{k+1}^T \tilde{A}_{k+1}\right\} - tr\left\{\tilde{A}_k^T \tilde{A}_k\right\}. \tag{17}$$

Substituting the parameter and state error dynamics (12) and (15) into (17) yields

$$\begin{aligned}\Delta L_{o,k} = &\begin{pmatrix} A_s \tilde{x}_k + \tilde{A}_k \hat{x}_k \\ +Dd_k \end{pmatrix}^T \Lambda_1 \begin{pmatrix} A_s \tilde{x}_k + \tilde{A}_k \hat{x}_k \\ +Dd_k \end{pmatrix} - \tilde{x}_k^T \Lambda_1 \tilde{x}_k \\ &+tr\left\{\left(\tilde{A}_k - \beta_1 \frac{\hat{x}_k \tilde{x}_{k+1}^T}{\left\|\hat{x}_k\right\|^2 + 1}\right)^T \left(\tilde{A}_k - \beta_1 \frac{\hat{x}_k \tilde{x}_{k+1}^T}{\left\|\hat{x}_k\right\|^2 + 1}\right) - \tilde{A}_k^T \tilde{A}_k\right\}.\end{aligned} \tag{18}$$

Apply Cauchy-Schwartz (C-S) inequality and (18) becomes

$$\begin{aligned}\Delta L_{o,k} \le &2\left(A_s \tilde{x}_k + \tilde{A}_k \hat{x}_k\right)^T \Lambda_1 \left(A_s \tilde{x}_k + \tilde{A}_k \hat{x}_k\right) + 2\left\|D^T \Lambda_1 D\right\| d_M^2 \\ &-\tilde{x}_k^T \Lambda_1 \tilde{x}_k + tr\left\{-2\beta_1 \frac{\tilde{A}_k^T \hat{x}_k \tilde{x}_{k+1}^T}{\left\|\hat{x}_k\right\|^2 + 1} + \beta_1^2 \frac{\tilde{x}_{k+1} \hat{x}_k^T \hat{x}_k \tilde{x}_{k+1}^T}{\left(\left\|\hat{x}_k\right\|^2 + 1\right)^2}\right\}.\end{aligned} \tag{19}$$

Since we have $tr\left\{v_1 v_2^T\right\} = v_2^T v_1$ for any vectors $v_1, v_2 \in \Re^{n\times 1}$, inequality (19) then becomes

$$\begin{aligned}\Delta L_{o,k} \le &1\left(1 - 4\left\|A_s\right\|^2\right)\left\|\Lambda_1\right\|\left\|\tilde{x}_k\right\|^2 + 4\left\|\Lambda_1\right\|\left\|\tilde{A}_k\right\|^2 \left\|\hat{x}_k\right\|^2 \\ &+2\left\|D^T \Lambda_1 D\right\| d_M^2 - 2\beta_1 \frac{\hat{x}_k^T \tilde{A}_k \tilde{x}_{k+1}}{\left\|\hat{x}_k\right\|^2 + 1} + \beta_1^2 \frac{\left\|\tilde{x}_k\right\|^2 \left\|\hat{x}_k\right\|^2}{\left(\left\|\hat{x}_k\right\|^2 + 1\right)^2}.\end{aligned} \tag{20}$$

Now, substituting the state error dynamics into (20) and applying C-S inequality yields

$$\begin{aligned}\Delta L_{o,k} \le &\left(1 - 4\left\|A_s\right\|^2\right)\left\|\Lambda_1\right\|\left\|\tilde{x}_k\right\|^2 + 4\left\|\Lambda_1\right\|\left\|\tilde{A}_k\right\|^2 \left\|\hat{x}_k\right\|^2 + 2\left\|D^T \Lambda_1 D\right\| d_M^2 - 2\beta_1 \frac{\hat{x}_k^T \tilde{A}_k A_s \tilde{x}_{k+1}}{\left\|\hat{x}_k\right\|^2 + 1} \\ &+2\beta_1 \frac{\left\|\hat{x}_k^T \tilde{A}_k D d_k\right\|}{\left\|\hat{x}_k\right\|^2 + 1} + 2\beta_1^2 \frac{\left\|\hat{x}_k\right\|^2 \left(A_s \tilde{x}_k + \tilde{A}_k \hat{x}_k\right)^T \left(A_s \tilde{x}_k + \tilde{A}_k \hat{x}_k\right) + \left\|\hat{x}_k\right\|^2 D^T D d_M^2}{\left(\left\|\hat{x}_k\right\|^2 + 1\right)^2}\end{aligned}$$

$$\leq\left(1-\frac{\beta_1}{2}\|A_s\|-4\|A_s\|^2\right)\|\Lambda_1\|\|\tilde{x}_k\|^2-2\beta_1\left(\begin{array}{c}1-\beta_1-\beta_1\|\hat{x}_k\|^2\\-\dfrac{1+\beta_1}{1+\|\hat{x}_k\|^2}\end{array}\right)\|\tilde{A}_k\|^2$$
$$+\left(2\|\Lambda_1\|+2\beta_1+\frac{\beta_1^2}{2}\right)\|D\|^2 d_M^2. \tag{21}$$

If (14) is satisfied, we have $\beta_1<\dfrac{2\left(1-4\|A_s\|^2\right)}{\|A_s\|}$, which is equivalent to $1-\dfrac{\beta_1}{2}\|A_s\|-4\|A_s\|^2>0$. On the other hand, (14) also implies that $\beta_1<\dfrac{\|\hat{x}_k\|^2}{\left(1+\|\hat{x}_k\|^2\right)^2+1}$, which can be expanded as $1-\beta_1-\beta_1\|\hat{x}_k\|^2-\dfrac{1+\beta_1}{1+\|\hat{x}_k\|^2}>0$. Therefore, by selecting the appropriate design parameter β_1 such that (14) is satisfied, we then can ensure the coefficients of $\|\tilde{x}_k\|^2$ and $\|\tilde{A}_k\|^2$ be negative. According to the standard Lyapunov theorem [27], the parameter estimation error, $\tilde{A}_k$, and state estimation error given by the observer $\tilde{x}_k$ are bounded within a small subset.

Remark 2: From (21) it can be seen that in the absence of disturbances, the parameter estimation error and the state estimation error will eventually converge to zero.

3.2. CONTROLLER DESIGN

Define the instant cost function as

$$r\left(x_k,u_k,k\right)=x_k^T P_k x_k+u_k^T R_k u_k, \tag{22}$$

where $P_k\in\Re^{n\times n}$ is a positive semi-definite symmetric time-varying weighting matrix and $R_k\in\Re^{+}$ stands for the weighting matrix of the control input. The objective of the controller

design is to determine a feedback control policy to minimize the following time-varying value function

$$J_k = x_N^T S_N x_N + \sum_{i=k}^{N-1} r\left(x_i, u_i, i\right). \tag{23}$$

with N being the final time instant. It is known [28] that the finite-horizon optimal control input, u_k^*, can be obtained by solving the Riccati equation (RE)

$$S_k = A^T\left(S_{k+1} - S_{k+1}B\left(B^T S_{k+1}B + R_k\right)^{-1} B^T S_{k+1}\right)A + P_k. \tag{24}$$

Accordingly, the optimal input is given by

$$u_k^* = -K_k^* x_k = -\left(B^T S_{k+1}B + R_k\right)^{-1} B^T S_{k+1}Ax_k. \tag{25}$$

However, the RE cannot be solved in this case since the system dynamics are unknown. To address this issue, we will use a Q-learning adaptive approach to estimate the value function and further to compute the controller gain.

Define the optimal action dependent value function as

$$\begin{aligned} &Q\left(x_k, u_k, N-k\right) \\ &= r\left(x_k, u_k, k\right) + J_{k+1} \triangleq \begin{bmatrix} x_k \\ u_k \end{bmatrix}^T G_k \begin{bmatrix} x_k \\ u_k \end{bmatrix}. \end{aligned} \tag{26}$$

Rewrite the Bellman equation as

$$\begin{aligned} &r\left(x_k, u_k, k\right) + J_{k+1} \\ &= \begin{bmatrix} x_k \\ u_k \end{bmatrix}^T \begin{bmatrix} P_k & 0 \\ 0 & R_k \end{bmatrix} \begin{bmatrix} x_k \\ u_k \end{bmatrix} + \left(Ax_k + Bu_k\right)^T S_{k+1}\left(Ax_k + Bu_k\right) \\ &= \begin{bmatrix} x_k \\ u_k \end{bmatrix}^T \begin{bmatrix} P_k + A^T S_{k+1}A & A^T S_{k+1}B \\ B^T S_{k+1}A & R_k + B^T S_{k+1}B \end{bmatrix} \begin{bmatrix} x_k \\ u_k \end{bmatrix}. \end{aligned} \tag{27}$$

Combining (26) and (27) yields

$$G_k = \begin{bmatrix} P_k + A^T S_{k+1} A & A^T S_{k+1} B \\ B^T S_{k+1} A & R_k + B^T S_{k+1} B \end{bmatrix} \triangleq \begin{bmatrix} G_k^{xx} & G_k^{xu} \\ G_k^{ux} & G_k^{uu} \end{bmatrix}. \tag{28}$$

Therefore the optimal control input can be derived from (25) and (28), which is given by $u_k^* = \left(G_k^{uu}\right)^{-1} G_k^{ux} x_k.$ (29)

It is important to note that one can compute the control input immediately from the matrix G_k , even though the system dynamics are unknown. Before proceeding, the following assumption is required.

Assumption 2 [29]: The slowly time-varying Q-function $Q(x_k, u_k, N-k)$ can be expressed as the linear-in-the-unknown parameters (LIP).

With 02, we express $Q(x_k, u_k, N-k)$ in the following form

$$Q(x_k, u_k, N-k) = z_k^T G_k z_k \triangleq g_k^T \overline{z}_k, \tag{30}$$

where $z_k \triangleq \begin{bmatrix} x_k^T & u_k^T \end{bmatrix}^T$, $\overline{z}_k$ is the Kronecker product quadratic polynomial basis vector of z_k and g_k is a vector generated by stacking the columns of G_k into a one-column vector with the summed off-diagonal elements. Now the smooth and uniformly piecewise-continuous function g_k can be represented as

$$g_k = \theta^T \varphi(N-k), \tag{31}$$

where $\theta \in \Re^{L \times L}$ with $L = n(n-1)/2$ is the target parameter vector and $\varphi(N-k)$ is the basis function matrix defined as $\left[\varphi(N-k)\right]_{i,j} = \exp\left(-\tanh(N-k)^{L+1-j}\right)$. Then the estimated value of target parameter is given by $\hat{g}_k = \hat{\theta}_k^T \varphi(N-k)$, (32)

where $\hat{\theta}_k$ is the estimated value of target parameter vector θ. Combine (30) with (32) and then the estimated value function is given by

$$\hat{Q}\left(x_k, u_k, N-k\right) = \hat{\theta}_k^T \varphi\left(N-k\right)\overline{z}_k \triangleq \hat{\theta}_k^T \breve{z}_k, \tag{33}$$

where $\breve{z}_k \triangleq \varphi\left(N-k\right)\overline{z}_k$ is the regression function satisfying $\breve{z}_k = 0$ for $\overline{z}_k = 0$. Accordingly, the control input using the estimated value function becomes

$$u_k = \left(\hat{G}_k^{uu}\right)^{-1} \hat{G}_k^{ux} x_k. \tag{34}$$

Note that if $\hat{G}_k^{uu}$ is singular then it is replaced by R_k. Then by using the adaptive observer (11), the Bellman error is given by

$$\begin{aligned} e_{b,k+1} &= \begin{bmatrix} \hat{x}_k \\ u_k \end{bmatrix}^T \begin{bmatrix} P_k + \hat{A}_k^T \hat{S}_{k+1} \hat{A}_k & \hat{A}_k^T \hat{S}_{k+1} B \\ B^T \hat{S}_{k+1} \hat{A}_k & R_k + B^T \hat{S}_{k+1} B \end{bmatrix} \begin{bmatrix} \hat{x}_k \\ u_k \end{bmatrix} \\ &- \hat{x}_k^T \hat{S}_k \hat{x}_k + 2\left(\hat{A}_k \hat{x}_k + B u_k\right)^T \hat{S}_{k+1} A_m \tilde{x}_k - \tilde{x}_k^T A_m^T \hat{S}_{k+1} A_m \tilde{x}_k + \left(\hat{\theta}_k^T \varphi(0) - g_N\right) I_v \\ &= -\hat{\theta}_k^T \Delta\breve{z}_k + r\left(\hat{x}_k, u_k, k\right) - \tilde{\theta}_k^T \varphi(0) I_v, \end{aligned} \tag{35}$$

where $\Delta\breve{z}_k \triangleq \breve{z}_k - \breve{z}_{k-1}$ and $I_v \triangleq [1,...,1] \in \Re^{1\times L}$.

Let $\sigma_k \triangleq \Delta\breve{z}_k - \varphi(0) I_v$ and $\bar{\varphi}\left(x_k\right) \triangleq kron\left(\left[x_k, u_k\right]\right)$ and $\bar{\varphi}\left(\hat{x}_k\right) \triangleq kron\left(\left[\hat{x}_k, u_k\right]\right)$ with $kron(\cdot)$ being the quadratic polynomial of the Kronecker product, then (35) can be rewritten as

$$e_{b,k+1} = \tilde{\theta}_k^T \sigma_k + \theta^T \left(\bar{\varphi}\left(x_k\right) - \bar{\varphi}\left(\hat{x}_k\right)\right) + r\left(x_k, u_k, k\right) - r\left(\hat{x}_k, u_k, k\right). \tag{36}$$

The update law for the value function estimator is given by

$$\hat{\theta}_{k+1} = \hat{\theta}_k + \beta_2 \frac{\sigma_k e_{b,k+1}}{\left\|\sigma_k\right\|^2 + 1}, \tag{37}$$

where $\beta_2 > 0$ is the tuning rate.

Then the error dynamics for $\hat{\theta}_k$ becomes

$$\tilde{\theta}_{k+1} = \tilde{\theta}_k - \beta_2 \frac{\sigma_k e_{b,k+1}}{\|\sigma_k\|^2 + 1}. \tag{38}$$

Now we are ready to introduce the boundedness of the closed-loop system.

Theorem 2 (Closed-loop System Stability): Consider the network traffic represented as a flow at the bottleneck node described by (9). Let the adaptive observer be described by (11) with the update law given by (13). Let the control input be given by (34) with the estimated value function tuned by (37) with $0 < \beta_2 < 1/5$. Then in the presence of bounded disturbances ($|d_k| \le d_M$) and in the absence of network attacks ($w_k = 0$), the parameter estimation error $\tilde{A}_k$, the state estimation error $\tilde{x}_k$, the value function estimation error $\tilde{\theta}_k$, and the system state vector x_k are all UB.

Proof: Define the Lyapunov function as

$$L_{s,k} = x_k^T x_k + \alpha_1 tr\left\{\tilde{\theta}_k^T \tilde{\theta}_k\right\} + \alpha_2 L_{o,k} \tag{39}$$

where $L_{o,k}$ is defined in (16). Then the first difference of the Lyapunov function is given by

$$\begin{aligned} \Delta L_{s,k} &= \left\| Ax_k + Bu_k^* - Bu_k^* + Bu_k + Dd_k \right\|^2 - \|x_k\|^2 + \alpha_2 \Delta L_{o,k} \\ &+ \alpha_1 tr\left\{ \left(\tilde{\theta}_k - \beta_2 \frac{\sigma_k e_{b,k+1}}{\|\sigma_k\|^2 + 1} \right)^T \left(\tilde{\theta}_k - \beta_2 \frac{\sigma_k e_{b,k+1}}{\|\sigma_k\|^2 + 1} \right) - \tilde{\theta}_k^T \tilde{\theta}_k \right\}. \end{aligned} \tag{40}$$

Applying C-S inequality and expand the last term in (40), we have

$$\begin{aligned} \Delta L_{s,k} &\le 2\left\| Ax_k + Bu_k^* \right\|^2 + 4\|B\|^2 \left\| u_k^* - u_k \right\|^2 + 4\|D\|^2 d_M^2 - \|x_k\|^2 \\ &+ \alpha_1 tr\left\{ -2\beta_2 \frac{\tilde{\theta}_k^T \sigma_k e_{b,k+1}}{\|\sigma_k\|^2 + 1} + \beta_2^2 \frac{e_{b,k+1}^T \sigma_k^T \sigma_k e_{b,k+1}}{\left(\|\sigma_k\|^2 + 1\right)} \right\} + \alpha_2 \Delta L_{o,k}, \end{aligned} \tag{41}$$

Note that $u_k^* - u_k = K_k^* x_k - \hat{K}_k x_k \triangleq \tilde{K}_k x_k$ and $\left\|\tilde{K}_k\right\| \le \varsigma_K \left\|\tilde{\theta}_k\right\|$ where ς_K is the positive Lipschitz constant. Then (41) becomes

$$\begin{aligned}\Delta L_{s,k} \le\ & 2\left\|Ax_k + Bu_k^*\right\|^2 + 4\|B\|^2 \varsigma_K^2 \left\|\tilde{\theta}_k\right\|^2 \|x_k\|^2 + 4\|D\|^2 d_M^2 - \|x_k\|^2 \\ & + \alpha_1 tr\left\{-2\beta_2 \frac{\tilde{\theta}_k^T \sigma_k e_{b,k+1}}{\|\sigma_k\|^2 + 1} + \beta_2^2 \frac{e_{b,k+1}^T \sigma_k^T \sigma_k e_{b,k+1}}{\left(\|\sigma_k\|^2 + 1\right)}\right\} + \alpha_2 \Delta L_{o,k},\end{aligned} \tag{42}$$

Since the closed loop system (9) with the optimal control input u^* satisfies $\left\|Ax_k + Bu_k^*\right\| \le \rho \|x_k\|^2$ with $0 < \rho < 1/2$ [1], we then have

$$\begin{aligned}\Delta L_{s,k} \le\ & -(1-2\rho)\|x_k\|^2 - 4\|B\|^2 \varsigma_c^2 \left\|\tilde{\theta}_k\right\|^2 - \left(\frac{2\alpha_1 \beta_2^2 \theta_M^2 \left(\varsigma_{\bar{\varphi}}^2 + \varsigma_r^2\right)}{\|\sigma_k\|^2 + 1} + 4B^2 K_M^2\right)\|\tilde{x}_k\|^2 \\ & -2\alpha_1 \beta_1 \left(1 - \beta_1 - \beta_1 \|\hat{x}_k\|^2 - \frac{1+\beta_1}{1+\|\hat{x}_k\|^2}\right)\left\|\tilde{A}_k\right\|^2 + \Psi_d.\end{aligned} \tag{43}$$

where $\alpha_1 \triangleq 8B^2 \varsigma_K^2 / \beta_2 \left(1 - \frac{1}{\|\sigma_k\|^2 + 1} - 5\beta_2\right)$, $\Psi_d \triangleq \left(4 + 2\|\Lambda_1\| + 2\beta_1 + \frac{\beta_1^2}{2}\right)\|D\|^2 d_M^2$

$\alpha_2 \triangleq \left(\begin{array}{l}\dfrac{4\alpha_1 \beta_2^2 \theta_M^2 \left(\varsigma_{\bar{\varphi}}^2 + \varsigma_r^2\right)}{\|\sigma_k\|^2 + 1} \\ +8B^2 K_M^2\end{array}\right) / \left(\left(1 - \dfrac{\beta_1}{2}\|A_s\| - 4\|A_s\|^2\right)\|\Lambda_1\|\right)$, and $\varsigma_{\bar{\varphi}}$ and ς_r are Lipschitz constants such that $\left\|\bar{\varphi}(x_k) - \bar{\varphi}(\hat{x}_k)\right\| \le \varsigma_{\bar{\varphi}} \|\tilde{x}_k\|$ and $\left\|\begin{array}{l} r(x_k, u_k, k) \\ -r(\hat{x}_k, u_k, k)\end{array}\right\| \le \varsigma_r \|\tilde{x}_k\|$.

Therefore, the parameter estimation error, $\tilde{A}_k$, state estimation error given by the observer $\tilde{x}_k$, the value function estimation error $\tilde{\theta}_k$, and the system state vector x_k are bounded within a small subset.

4. NETWORK FLOW ATTACK DETECTION SCHEME

In this section, we first introduce the adversary models of three typical flow-targeted network attacks. Next, we develop the network attack scheme based on the observer designed in the previous section. The detectability condition is also given under which certain types of attacks can be detected. After attack detecting, an observer is proposed to estimate its flow.

4.1. ADVERSARY MODEL

Cyber-attacks are multifarious but they all target at one or more of the three fundamental properties of information and services: confidentiality, integrity, and availability, often known as CIA [26]. Confidentiality-targeted attacks are usually defended by encryption techniques and therefore in this paper, we only concern about attacks that impair the integrity and availability. Specifically, in the context of flow management, this paper deals with attacks that either inject false data or drop/block authentic data. Three types of such attacks are considered as examples.

Jamming Attack: The jamming attacker aims at creating traffic congestion by placing jammers that consistently inject data into the link. Assuming the attacking strength (number of jammers) increases linearly, then this type of attack can be modeled by [27]

$$w_k = 1 - e^{-\beta k} \ , \tag{44}$$

where k, ω_k and β is the time, percentage of injected data, and the network-related coefficient, respectively. Jamming attack is plotted in Figure 4.1.

Black hole Attack: If the attacker manages to compromise one or more nodes in the routing path from the source to the destination, then a black hole attack has been launched. As a result, part of the data (depending on the attack strength) would be discarded. Assuming the attack strength (number of black holes) increases linearly, then the black hole attack can be modeled by a linear equation [28] given by

$$w_k = 1 - \beta k \ , \tag{45}$$

where k, ω_k and β is the attack strength (number of black holes), percentage of dropped data, and the network-related coefficient, respectively and it is plotted in Figure 4.2.

Minimum Rate DoS Streams Attack: Instead of continuously injecting data, false data is periodically injected into the network, in order to avoid router-based mechanisms that detect high rate flows. In this way, the attacker attempts to minimize their exposure to detection mechanisms. A typical minimum rate DoS stream attack is described by [29]

$$w_k = \begin{cases} n_1, & \text{for } t \in \left[k\tilde{T}, k\tilde{T} + p_1 \right]; \\ n_2, & \text{for } t \in \left[k\tilde{T} + p_1, k\tilde{T} + p_2 \right]; \\ 0, & \text{for } t \in \left[k\tilde{T} + p_2, (k+1)\tilde{T} \right], \end{cases} \tag{46}$$

where $n_1, n_2, \eta, p_{1,} p_2$,and $\tilde{T}$ is the first attack strength, second attack strength, packet drop rate, first attack duration, second attack end time, and total attack period, respectively. The DOS stream attack is plotted in Figure 4.3. Next, an attack detection scheme is introduced.

4.2. ATTACK DETECTION AND ESTIMATION SCHEME

In this section, we will present the attack detectability condition followed by the detection scheme performance. Theorem 2 shows that without the presence of the attacks, the system is stable and the estimation error (or the detection residue) is UB. In the next

theorem, the attack is introduced and a theoretic condition is derived under which the attack can be detected.

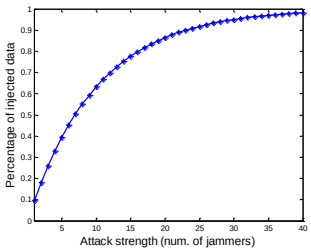


Figure 4.1. Jamming attack.

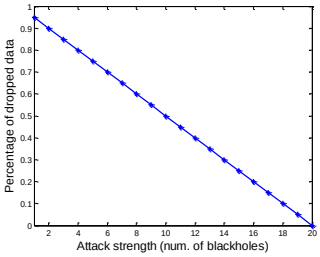


Figure 4.2. Black hole attack.

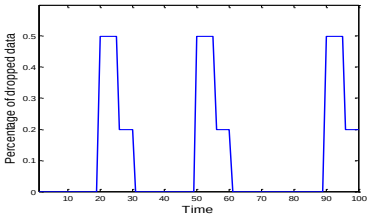


Figure 4.3. Minimum rate DoS streams attack.

Theorem 3 (Network Attack Detectability Condition): Consider the network traffic represented as a flow at the bottleneck node described by (9). Let the adaptive observer be described by (11) with the update law given by (13). Let the control input be given by (34) with the estimated value function tuned by (37). Assume the attack is launched at $t = k_0 \geq 0$, after the convergence of the system state x_k, matrix A estimation error $\tilde{A}_k$, and state estimation error $\tilde{x}_k$. Then the attack is detectable at time $t = k \geq k_0 + 1$ if the injected (dropped) traffic flow $w(x_k)$ into (from) the link satisfies

$$\left\| \sum_{i=k_0}^{k-1} A_m^{k-k_0-i-1} W w(x_i) \right\| > \Upsilon_k + \left\| A_m^{k-k_0} \tilde{x}_{k_0} + \sum_{i=k_0}^{k-1} A_m^{k-k_0-i-1} \tilde{A}_i x_i \right\|, \tag{47}$$

where $\Upsilon_k \triangleq \Psi_d / \left(2\alpha_1 \beta_2^2 \theta_M^2 \left(\varsigma_{\bar{\varphi}}^2 + \varsigma_r^2 \right) / \left(\|\sigma_k\|^2 + 1 \right) + 4B^2 K_M^2 \right)$ with Ψ_d defined in (43).

Proof: According to (43) derived in Theorem 2, the estimation error of the system state under healthy condition is bounded by

$$\left\|\tilde{x}_k\right\| \le \Upsilon_k . \tag{48}$$

With the presence of attacks, the error dynamic of the system states becomes

$$\tilde{x}_{k+1} = A_m \tilde{x}_k + \tilde{A}_k x_k + W w\left(x_k\right). \tag{49}$$

The solution of $\tilde{x}_{k+1}$ with the initial condition of $\tilde{x}_{k_0}$ is given by

$$\tilde{x}_k = A_m^{k-k_0}\tilde{x}_{k_0} + \sum_{i=k_0}^{k-1} A_m^{k-k_0-i-1}\tilde{A}_i x_i + \sum_{i=k_0}^{k-1} A_m^{k-k_0-i-1} W w\left(x_i\right). \tag{50}$$

Therefore, if the attack input $w\left(x_k\right)$ is large enough such that (36) is satisfied, by using triangle inequality we have

$$\begin{aligned} \left\|\tilde{x}_k\right\| &= \left\| \begin{matrix} A_m^{k-k_0}\tilde{x}_{k_0} + \sum_{i=k_0}^{k-1} A_m^{k-k_0-i-1}\tilde{A}_i x_i \\ + \sum_{i=k_0}^{k-1} A_m^{k-k_0-i-1} W w\left(x_i\right) \end{matrix} \right\| \\ &\ge \left\| \sum_{i=k_0}^{k-1} A_m^{k-k_0-i-1} W w\left(x_i\right) \right\| - \left\| \begin{matrix} A_m^{k-k_0}\tilde{x}_{k_0} + \\ \sum_{i=k_0}^{k-1} A_m^{k-k_0-i-1}\tilde{A}_i x_i \end{matrix} \right\| > \Upsilon_k . \end{aligned} \tag{51}$$

Note that the inequality (47) presents a sufficient condition under which certain types of attacks can be detected. However it is not the way how the attack is detected in practice. Instead, the estimation error or the detection residue is constantly monitored and the attack is detected when the residue exceeds the bound given by (48).

Upon detecting the attack, it is of interest to know how much flow has been injected or dropped by the attacker. For this purpose, we propose to add an adaptive term to the observer (11) to estimate the attack input. Before we proceed, the following assumption that is widely used in adaptive control [35] is made.

Assumption 3: Assume the attack input $w(x_k)$ is bounded by $|w(x_k)| \le w_M$ and it can be expressed as $w(x_k) = \theta_w^T \varphi_w(x_k)$, where $\theta_w \in \Re^{n\times 1}$ is an unknown constant vector bounded by $\|\theta_w\| \le \theta_{w,M}$ and the regression function $\varphi_w : \Re^{n\times 1} \to \Re^{n\times 1}$ is known and bounded by $\|\varphi_w(x_k)\| \le \varphi_{w,M}$.

In the presence of bounded attacks, the system states dynamic becomes

$$x_{k+1} = \tilde{A}_k x_k + A_s x_k + Dd_k + Ww_k . \tag{52}$$

Define the new observer with attack estimation as

$$\hat{x}_{k+1} = \hat{A}_k \hat{x}_k - A_m(x_k - \hat{x}_k) + Bu_k + W\hat{w}_k , \tag{53}$$

where $\hat{w}_k \triangleq \hat{\theta}_{w,k}^T \varphi_w(x_k)$ with $\hat{\theta}_w$ being the estimation of the unknown parameter θ_w is the estimated attack input. Combining (53) with (52) yields the state estimation error dynamics with attack estimation

$$\tilde{x}_{k+1} = A_s \tilde{x}_k + \tilde{A}_k \hat{x}_k + Dd_k + W\tilde{w}_k , \tag{54}$$

where $\tilde{w}_k \triangleq w_k - \hat{w}_k$ is the estimation error of the unknown attack input.

The next theorem introduces the adaptive update law for the estimation of attack input such the parameter estimation error of attack input $\tilde{\theta}_{w,k}$, the system state x_k, matrix A estimation error $\tilde{A}_k$, and state estimation error given by the observer $\tilde{x}_k$ are all UB.

Theorem 4 (Network Attack Estimation): Consider the network traffic represented as a flow at the bottleneck node described by (9) in the presence of bounded attacks. Attacks can be detected when the network detection residual exceeds a predefined threshold given by (48).

Upon detecting the attack, consider the observer (53) with the following adaptive update law for the estimation of unknown attack flow input

$$\hat{\theta}_{k+1} = \hat{\theta}_k - \beta_4 \tilde{x}_k^T \hat{A}_k^T \varphi_w(x_k) - \beta_3 \left| 1 - \beta_4 \varphi_w^T(x_k) \varphi_w(x_k) \right| \hat{\theta}_k, \tag{55}$$

where $\beta_3, \beta_4 \in \Re^+$ and $\bar{K} \in \Re^{n \times n}$ are design parameters. Then by selecting the appropriate design parameters, the parameter estimation error of attack input $\tilde{\theta}_{w,k}$, states estimation error $\tilde{x}_k$, and matrix A estimation error $\tilde{A}_k$ are all UB.

Proof: According to (55) with the fact that $W^T W = 1$, the estimation error dynamic of w_k is given by

$$\begin{aligned} \tilde{\theta}_{w,k} &= \left(1 - \beta_3 \left| 1 - \beta_4 \varphi_w^T(x_k) \varphi_w(x_k) \right| \right) \tilde{\theta}_{w,k} \\ &+ \beta_4 \tilde{x}_k^T \hat{A}_k^T \varphi_w(x_k) + \beta_3 \left| 1 - \beta_4 \varphi_w^T(x_k) \varphi_w(x_k) \right| \theta_w. \end{aligned} \tag{56}$$

Now select the Lyapunov function as

$$L_k = L_{o,k} + L_{a,k} \tag{57}$$

where $V_{o,k}$ is defined in (16) and $L_{a,k} \triangleq \tilde{\theta}_{w,k}^T \tilde{\theta}_{w,k}$.

Substituting estimation error dynamics of the system parameters and states (15) and (54) into $L_{o,k}$, we then have

$$\begin{aligned} &\Delta L_{o,k} \\ &= \begin{pmatrix} A_s \tilde{x}_k + \tilde{A}_k \hat{x}_k \\ + D d_k + W \tilde{w}_k \end{pmatrix}^T \Lambda_1 \begin{pmatrix} A_s \tilde{x}_k + \tilde{A}_k \hat{x}_k \\ + D d_k + W \tilde{w}_k \end{pmatrix} - \tilde{x}_k^T \Lambda_1 \tilde{x}_k \\ &+ tr \left\{ \left(\tilde{A}_k - \beta_1 \frac{\hat{x}_k \tilde{x}_{k+1}^T}{\left\| \hat{x}_k \right\|^2 + 1} \right)^T \left(\tilde{A}_k - \beta_1 \frac{\hat{x}_k \tilde{x}_{k+1}^T}{\left\| \hat{x}_k \right\|^2 + 1} \right) - \tilde{A}_k^T \tilde{A}_k \right\}. \end{aligned} \tag{58}$$

Applying C-S inequality and expanding the last term we have

$$\Delta L_{o,k} \le 2\left(A_s\tilde{x}_k + \tilde{A}_k\hat{x}_k\right)^T \Lambda_1\left(A_s\tilde{x}_k + \tilde{A}_k\hat{x}_k\right) + 4\left\|D^T\Lambda_1 D\right\| d_M^2 + 4\tilde{w}_k^T W^T\Lambda_1 W\tilde{w}_k - \tilde{x}_k^T\Lambda_1\tilde{x}_k$$
$$-2\beta_1\frac{\hat{x}_k^T\tilde{A}_k\tilde{x}_{k+1}}{\left\|\hat{x}_k\right\|^2+1} + \beta_1^2\frac{\left\|\tilde{x}_k\right\|^2\left\|\hat{x}_k\right\|^2}{\left(\left\|\hat{x}_k\right\|^2+1\right)^2}$$

$$\le\left(1-4\left\|A_s\right\|^2\right)\left\|\Lambda_1\right\|\left\|\tilde{x}_k\right\|^2 + 4\left\|\Lambda_1\right\|\left\|\tilde{A}_k\right\|^2\left\|\hat{x}_k\right\|^2 + 4\left\|D^T\Lambda_1 D\right\| d_M^2 + 4\lambda_{\max}\left\{W^T\Lambda_1 W\right\}\tilde{w}_k^2$$
$$-2\beta_1\frac{\hat{x}_k^T\tilde{A}_k A_s\tilde{x}_{k+1}}{\left\|\hat{x}_k\right\|^2+1} + 2\beta_1\frac{\left\|\hat{x}_k^T\tilde{A}_k\left(Dd_k + Ww_k\right)\right\|}{\left\|\hat{x}_k\right\|^2+1}$$
$$+2\beta_1^2\frac{\left\|\hat{x}_k\right\|^2\left(A_s\tilde{x}_k + \tilde{A}_k\hat{x}_k\right)^T\left(A_s\tilde{x}_k + \tilde{A}_k\hat{x}_k\right) + 2\left\|\hat{x}_k\right\|^2\left(d_M^2 + w_M^2\right)}{\left(\left\|\hat{x}_k\right\|^2+1\right)^2}$$

$$\le\left(1-\frac{\beta_1}{2}\left\|A_s\right\| - 4\left\|A_s\right\|^2\right)\left\|\Lambda_1\right\|\left\|\tilde{x}_k\right\|^2 - 2\beta_1\left(1-\beta_1-\beta_1\left\|\hat{x}_k\right\|^2 - \frac{1+\beta_1}{1+\left\|\hat{x}_k\right\|^2}\right)\left\|\tilde{A}_k\right\|^2$$
$$+\left(4\left\|\Lambda_1\right\| + 2\beta_1 + \beta_1^2\right)d_M^2 + \left(2\beta_1+\beta_1^2\right)w_M^2. \tag{59}$$

Now substituting the error dynamics of the $\hat{w}_k$ into $L_{a,k}$ yields

$$\Delta L_{a,k} = \left(\left(1-\beta_5\right)\tilde{\theta}_{w,k} + \beta_4\tilde{x}_k^T\hat{A}_k^T\varphi_w\left(x_k\right) + \beta_5\theta_w\right)^T$$
$$\times\left(\left(1-\beta_5\right)\tilde{\theta}_{w,k} + \beta_4\tilde{x}_k^T\hat{A}_k^T\varphi_w\left(x_k\right) + \beta_5\theta_w\right) - \tilde{w}_k^T\tilde{w}_k. \tag{60}$$

where $\beta_5 \triangleq \beta_3\left|1-\beta_4\varphi_w^T\left(x_k\right)\varphi_w\left(x_k\right)\right|\hat{\theta}_{w,k}$.

Apply C-S inequality yields

$$\Delta L_{a,k} \le 2\tilde{\theta}_{w,k}^2 - 6\beta_5\tilde{\theta}_{w,k}^2 + 3\beta_5^2\left(\tilde{\theta}_{w,k}^2 + \theta_w^2\right) + 3\beta_4^2\left(\bar{K}\tilde{x}_k^T A_s^T\varphi_w\left(x_k\right)\right)^T\left(\bar{K}\tilde{x}_k^T A_s^T\varphi_w\left(x_k\right)\right)$$
$$\le -\left(-2+6\beta_5-3\beta_5^2\right)\tilde{\theta}_{w,k}^2 + 3\beta_4^2\lambda_{\max}^2\left\{A_s\right\}\varphi_{w,M}^2\left\|\bar{K}\right\|^2\left\|\tilde{x}_k\right\|^2 + 2\beta_5^2\theta_{w,M}^2. \tag{61}$$

Therefore, combining (59) and (60) yields the total first difference of the Lyapunov function, which is given by

$$
\begin{aligned}
&\Delta L_k = \Delta L_{o,k} + \Delta L_{a,k} \\
&\le \left(1 - \frac{\beta_1}{2}\|A_s\| - 4\|A_s\|^2 - 3\beta_4^2 \lambda_{\max}^2\{A_s\}\varphi_{w,M}^2 \|\bar{K}\|^2 \|\Lambda_1\|^{-1}\right)\|\Lambda_1\|\|\tilde{x}_k\|^2 \\
&-2\beta_1\left(1 - \beta_1 - \beta_1\|\hat{x}_k\|^2 - \frac{1+\beta_1}{1+\|\hat{x}_k\|^2}\right)\|\tilde{A}_k\|^2 - \left(-2 + 6\beta_5 - 3\beta_5^2\right)\tilde{\theta}_{w,k}^2 \\
&+\left(4\|\Lambda_1\| + 2\beta_1 + \beta_1^2\right)d_M^2 + \left(\left(2\beta_1 + \beta_1^2\right)\varphi_{w,M}^2 + 2\beta_5^2\right)\theta_{w,M}^2 .
\end{aligned}
\tag{62}
$$

Therefore, by selecting the appropriate parameters such that (14) and $1-\sqrt{3}/3 < \beta_5 < 1+\sqrt{3}/3$ hold, the estimation error of attack input $\tilde{w}_k$, states estimation error $\tilde{x}_k$, and matrix A estimation error $\tilde{A}_k$ are all UB.

5. ATTACK DETECTION FOR THE PHYSICAL SYSTEM

In this section, we first revisit a stochastic event-triggered optimal control scheme [14] for a class of linear systems in the presence network-induced delays and packet losses. An event triggered control scheme is proven to reduce network traffic which might help to mitigate congestion in the presence of attacks in the event that attacks increase traffic flow. Next, since a large delay and packet loss rate could lead to the instability of the system, the maximum overall delay and packet loss that the physical system can tolerate is derived. At last, we present the proposed a detection scheme for sensor/actuator attacks on the physical system.

5.1. PHYSICAL SYSTEM DYNAMICS

Consider the stochastic linear continuous-time system with network-induced delays and packet losses described by

$$\dot{\bar{x}}_p(t) = \bar{A}_p \bar{x}_p(t) + \chi_{ca}(t)\bar{B}_p \bar{u}_p(t-\tau(t)) + \chi_{ca}^{'}(t)\bar{w}_p\left(t-\tau^{'}(t)\right), \tag{63}$$

where $\bar{x}_p(t) \in \Re^n$, $\bar{u}_p(t) \in \Re^m$, and $\bar{w}_p(t) \in \Re^n$ is the system state, controller input, and attack flow input vector, respectively. The system matrices $\bar{A}_p \in \Re^{n\times n}$ and $\bar{B}_p \in \Re^{n\times m}$ are considered as unknown. The subscript " p " standing for "physical system" is utilized to differentiate the variable used to denote the network. In particular, the notation $\tau(t)$ and $\tau^{'}(t)$ stand for the network-induced sensor-to-controller delay which is bounded by $\tau(t) \le \tau_M$ and $\chi_{ca}(t)$ and $\chi_{ca}^{'}(t) \in \Re^{n\times n}$ are the packet loss indicators which equal to the identity matrix I_n when the packet is received and the null matrix when the packet is lost.

Remark 3: The term $\bar{w}_p(t)$ is used to characterize the change in system states caused by attacks on the sensors or actuators [34]. From the diagram of NCS in 0, it can be seen that if $\bar{w}_p(t)$ is the sensor attack input, then we have $\tau'(t) = \tau(t)$ and $\chi'_{ca}(t) = \chi_{ca}(t)$. On the other hand, if $\bar{w}_p(t)$ is the actuator attack input, we will have $\tau'(t) = 0$ and $\chi'_{ca} = I_n$ since the actuator-plant link does not rely on the networks.

Remark 4: It is important to note that although it appears from (63) that the attack affects the system states, this representation is not limited to the case where the attack targets at the states [34]. For instance, for any actuator attacks where the controller input is manipulated from u_p to $\bar{u}_p + \Delta\bar{u}_p$, the attack input term in (63) then becomes $\bar{B}_p \Delta\bar{u}_p$. Likewise, for any sensor attack where the state in the feedback loop is manipulated from $x_{p,k}$ to $x_{p,k} + \Delta x_{p,k}$, then the system dynamics becomes $x_{p,k+1} = \bar{A}_p x_{p,k} + \bar{B}_p K_{p,k}\left(x_{p,k} + \Delta x_{p,k}\right)$. In this case, the attack input becomes $w_{p,k} = \bar{B}_p K_{p,k} \Delta x_{p,k}$. Attacks on the physical systems can be detected if $\bar{w}_p(t)$ satisfies certain condition. This will be discussed later in Section 5.2 after the healthy case, i.e., $\bar{w}_p(t) = 0$.

Let the augmented state be defined as $x_{p,k} = [\bar{x}_{p,k}^T \quad \bar{u}_{p,k-1}^T \quad \cdots \quad \bar{u}_{p,k-\tau_M}^T]^T \in \Re^{n+\tau_M m}$ and discretizing system (42) within the sampling period $\left[kT_s, (k+1)T_s\right]$ yields the simplified system dynamics

$$x_{p,k+1} = A_p x_{p,k} + B_p u_{p,k} + W_p w_{p,k}, \tag{64}$$

where $u_{p,k}$ and $w_{p,k}$ are the discretized control input and attack input respectively and matrices A_p, B_p and W_p are defined in [12]. The following assumption is needed in order

to proceed.

Assumption 4: Let assumptions (1-4) presented [14] hold.

The event-triggered control (ETC) from [14] is adopted in this paper due to benefits mentioned before. Furthermore, unlike traditional event-triggered control schemes, the proposed approach in [14] utilizes the time-driven Q-learning along with the iterative parameter learning updates within the event-sampled instants to both improved efficiency of the optimal regulator and obtain a more generalized online Q-learning framework.

For the system dynamics(64), define the instant cost function as

$$r_p\left(x_{p,k},u_{p,k},k\right)=x_{p,k}^T P_{p,k}x_{p,k}+u_{p,k}^T R_{p,k}u_{p,k}, \tag{65}$$

where $P_{p,k}$ is a positive semi-definite matrix and $R_{p,k}$ is a positive define matrix. The objective of the controller design is to determine a feedback control policy to minimize the following value function

$$J_{p,k}=\underset{\tau,\gamma}{E}\left\{\frac{1}{2}\sum\nolimits_{i=k}^{\infty} r_p\left(x_{p,i},u_{p,i},i\right)\right\}. \tag{66}$$

Define the action-dependent Q-function as

$$Q\left(x_{p,k},u_{p,k}\right)=\underset{\tau,\gamma}{E}\left\{r\left(x_{p,k},u_{p,k}\right)+J_{p,k+1}\right\}=\underset{\tau,\gamma}{E}\left\{\begin{bmatrix}x_{p,k}\\u_{p,k}\end{bmatrix}^T G_{p,k}\begin{bmatrix}x_{p,k}\\u_{p,k}\end{bmatrix}\right\}. \tag{67}$$

From the Bellman equation, we have

$$\begin{bmatrix}x_{p,k}\\u_{p,k}\end{bmatrix}^T \underset{\tau,\gamma}{E}\left\{G_{p,k}\right\}\begin{bmatrix}x_{p,k}\\u_{p,k}\end{bmatrix}=\begin{bmatrix}x_{p,k}\\u_{p,k}\end{bmatrix}^T\begin{bmatrix}P_{p,k}+\underset{\tau,\gamma}{E}\left\{A_p^T S_{p,k+1}A_p\right\} & \underset{\tau,\gamma}{E}\left\{A_p^T S_{p,k+1}B_p\right\}\\ \underset{\tau,\gamma}{E}\left\{B_p^T S_{p,k+1}A\right\} & R_{p,k}+\underset{\tau,\gamma}{E}\left\{B_p^T S_{p,k+1}B_p\right\}\end{bmatrix}\begin{bmatrix}x_{p,k}\\u_{p,k}\end{bmatrix}. \tag{68}$$

where $\underset{\tau,\gamma}{E}\left\{G_{p,k}\right\} \triangleq \begin{bmatrix} \underset{\tau,\gamma}{E}\left\{G_{p,k}^{xx}\right\} & \underset{\tau,\gamma}{E}\left\{G_{p,k}^{xu}\right\} \\ \underset{\tau,\gamma}{E}\left\{G_{p,k}^{ux}\right\} & \underset{\tau,\gamma}{E}\left\{G_{p,k}^{uu}\right\} \end{bmatrix}$. The control input is given by

$$u_{p,k} = \underset{\tau,\gamma}{E}\left\{\left(G_{p,k}^{uu}\right)^{-1} G_{p,k}^{ux}\right\} x_{p,k} \ . \tag{69}$$

The Q-function in parametric form is given by

$$Q\left(x_{p,k}, u_{p,k}\right) = \underset{\tau,\gamma}{E}\left\{z_{p,k}^{T} G_{p,k} z_{p,k}\right\} = \underset{\tau,\gamma}{E}\left\{\Theta_k^{T} \xi_k\right\}, \tag{70}$$

where $z_{p,k} \triangleq \begin{bmatrix} \left(\gamma_k x_{p,k}\right)^{T} & u_{p,k}^{T} \end{bmatrix}^{T}$, ξ_k is the Kronecker product quadratic polynomial basis vector of $z_{p,k}$, and Θ_k is a vector generated by stacking the columns of $G_{p,k}$ into a one-column vector with the summed off-diagonal elements. The estimation of the optimal Q-function is given by

$$\hat{Q}\left(x_{p,k}, u_{p,k}\right) = \underset{\tau,\gamma}{E}\left\{z_{p,k}^{T} \hat{G}_{p,k} z_{p,k}\right\} = \underset{\tau,\gamma}{E}\left\{\hat{\Theta}_k^{T} \xi_k\right\}, \tag{71}$$

where $\hat{\Theta}_k$ is the estimation of the unknown expected target parameter Θ_k. In event-triggered control systems, the state vector is sent to the controller only when the trigger condition is violated. Let $\{k_l\}$ with $l \in \mathbb{N}$ and $k_0 = 0$ denote the sequence of event-trigger instants.

The state vector is held at the controller until the next sampling instant and it is expressed as $x_{p,k}^{e} = x_{p,k_l}$ for $k_l \le k \le k_{l+1}$. The event-sampled error is then given by

$$e_{ET,k} = x_{p,k} - x_{p,k}^{e} \ . \tag{72}$$

Accordingly, the estimated Q-function using $x_{p,k}^{e}$ becomes

$$\hat{Q}\left(x_{p,k}^{e}, u_{p,k}\right) = \underset{\tau,\gamma}{E}\left\{z_{p,k}^{e,T} \hat{G}_{p,k} z_{p,k}^{e}\right\} = \underset{\tau,\gamma}{E}\left\{\hat{\Theta}_k^{T} \xi_k^{e}\right\}. \tag{73}$$

where $z_{p,k}^e \triangleq \left[\left(\gamma_k x_{p,k}^e\right)^T \quad u_{p,k}^T\right]^T$ and ξ_k^e is the Kronecker product quadratic polynomial basis vector of $z_{p,k}^e$. Then the Bellman error with the event-sampled states is given by

$$e_{B,k} = \underset{\tau,\gamma}{E}\left\{r\left(x_{p,k}, u_{p,k}\right) + \hat{\Theta}_k^T \Delta\xi_k + \Xi_{s,k}\right\}, \tag{74}$$

where $\Xi_{s,k} \triangleq r\left(x_{p,k} - e_{ET,k}, u_{p,k}\right) - r\left(x_{p,k}, u_{p,k}\right) + \hat{\Theta}_k^T \begin{pmatrix} \Delta\xi_k^e - \\ \Delta\xi_k \end{pmatrix}$.

It can be seen from (74) that the Bellman error also depends on the event-sampled error $e_{ET,k}$. Therefore, the estimation of the optimal Q-function depends on the frequency of the event-sapling instants. With the event-sampled states, the estimated optimal control input is given by

$$u_{p,k} = -\left(\hat{G}_{p,k}^{uu}\right)^{-1} \hat{G}_{p,k}^{ux} x_{p,k}^e \ . \tag{75}$$

At the event-sampled event, the Q-function estimator (QFE) parameter vector $\hat{\Theta}_k$ is tuned by using the history data of the Bellman error (74) for a faster convergence. Define the auxiliary Bellman error as

$$\Xi_{B,k}^e \triangleq \Pi_k^e + \hat{\Theta}_k^T Z_k^e, \text{ for } k = k_l, \tag{76}$$

where $Z_k^e \triangleq \left[\Delta\xi_{k_l} \quad \Delta\xi_{k_{l-1}} \quad \cdots \quad \Delta\xi_{k_{l-v-1}}\right]$ and $\Pi_k^e \triangleq \left[r\left(x_{p,k_l}, u_{p,k_l}\right) \quad r\left(x_{p,k_{l-1}}, u_{p,k_{l-1}}\right) \quad \cdots \quad r\left(x_{p,k_{l-v-1}}, u_{p,k_{l-v-1}}\right)\right]$ with $v \in \Re^+$ being the number of past values. At the event-sampled instants, The QFE parameter vector $\hat{\Theta}_k$ is tuned with the following update law [V, 29]:

$$\hat{\Theta}_k = \hat{\Theta}_{k-1} + \frac{\Omega_{k-2} Z_{k-1}^e \Xi_{B,k-1}^{e^T}}{1 + Z_{k-1}^{e^T} \Omega_{k-2} Z_{k-1}^e}, \text{ for } k = k_l, \tag{77}$$

where

$$\Omega_k = \Omega_{k-1} + \frac{\Omega_{k-1} Z_{k-1}^{e} Z_{k-1}^{e^T} \Omega_{k-1}}{1 + Z_{k-1}^{e^T} \Omega_{k-1} Z_{k-1}^{e}}, \text{ for } k = k_l, \tag{78}$$

with $\Omega_0 = \eta_0 I$, $\eta_0 = 0$, a large positive value.

Within the time between two event-sampled event, parameters are updated iteratively in order to minimize the error calculated after previous event sampling instant. The update law for the QFE parameters is selected as

$$\hat{\Theta}_{k_l^j} = \hat{\Theta}_{k_l^{j-1}} + \frac{\Omega_{k_{l-2}^{j-2}} Z_{k_{l-1}^{j-1}} \Xi_{B,k_{l-1}^{j-1}}^{T}}{1 + Z_{k_{l-1}^{j-1}}^{T} \Omega_{k_{l-2}^{j-1}} Z_{k_{l-1}^{j-1}}} \text{ and} \tag{79}$$

$$\Omega_{k_l^j} = \Omega_{k_{l-1}^{j-1}} - \frac{\Omega_{k_{l-1}^{j-1}} Z_{k_{l-1}^{j-1}} Z_{k_{l-1}^{j-1}}^{T} \Omega_{k_{l-1}^{j-1}}}{1 + Z_{k_{l-1}^{j-1}}^{T} \Omega_{k_{l-1}^{j-1}} Z_{k_{l-1}^{j-1}}}, \tag{80}$$

where the superscript " j " denotes the iteration index.

Define the QFE estimation error as $\underset{\tau,\gamma}{E}\left\{\tilde{\Theta}_k\right\} \triangleq \underset{\tau,\gamma}{E}\left\{\Theta_k - \hat{\Theta}_k\right\}$ and then the error dynamics can be derived by using (77) and (79), which is given by

$$\underset{\tau,\gamma}{E}\left\{\tilde{\Theta}_{k_{l+1}}^{0}\right\} = \underset{\tau,\gamma}{E}\left\{\tilde{\Theta}_k^j + \frac{\Omega_k^j Z_k^{j,e} \Xi_{B,k}^{j,e^T}}{1 + Z_k^{j,e^T} \Omega_k^j Z_k^{j,e}}\right\}, \; k = k_l^0 \text{ and} \tag{81}$$

$$\underset{\tau,\gamma}{E}\left\{\tilde{\Theta}_{k_l}^{j+1}\right\} = \underset{\tau,\gamma}{E}\left\{\tilde{\Theta}_k^j + \frac{\Omega_k^j Z_k^{j,e} \Xi_{B,k}^{j,e^T}}{1 + Z_k^{j,e^T} \Omega_k^j Z_k^{j,e}}\right\}, \; k_l^0 < k < k_{l+1}^0. \tag{82}$$

The event-trigger condition design is critical because on one hand, excessive triggering clearly deviates from the original intention of reducing the data transmission. On the other hand, insufficient triggering will result in a regulation error, thus degrading the

performance and even leading to the instability of the system. Here, the event-trigger condition is given by [14]:

$$f\left(k\right)\le\lambda f\left(k_l+1\right),\ \forall k\in\left[k_l+1,k_{l+1}\right), \tag{83}$$

where $f\left(k\right)\triangleq x_{p,k}^T\Gamma x_{p,k}$ is a quadratic function with $\Gamma>0$ and $\lambda<1$. Now we are ready to introduce the QFE performance as well as the closed-loop system stability under healthy case where there are no attacks on the physical system.

Theorem 5 (Parameter Estimation and Stability) [14]: Consider the closed-loop system (64) in the absence of attacks on the physical system and the network. Let the control input be given by (75) with u_0 being an initial admissible control input. Suppose the QFE estimator vector is updated by using (77) at the event-sampled instants and (79) during the inter-sampling period. Select the event-trigger condition given by (83). Assume the regression vector $\xi_{k_l}^j$ satisfies the persistently exciting (PE) condition. Then there exists a constant $\gamma_{\min}>0$ such that both the state vector x_{p,k_l}^j and the QFE estimation error converge to zero asymptotically in the mean square. Moreover, the estimated Q-function $\hat{Q}\left(x_{p,k},u_{p,k}\right)\to\underset{\tau,\gamma}{E}\left\{Q^*\left(x_{p,k},u_{p,k}\right)\right\}$ and the estimated control input $u_{p,k}\to\underset{\tau,\gamma}{E}\left\{u_{p,k}^*\right\}$ with the event-sampled instants $k_l\to\infty$.

In the above analysis, we consider the case where the communication network is in healthy condition, i.e., the delays and packet losses are bounded by a small value. However, the delays and packet losses increase in the presence of attacks on the network and lead to instability of the physical system. Therefore, it is of interest to determine the maximum delays and packet losses that the physical system can tolerate.

Let $\left[k_l, \quad k_l + \varepsilon_{p,k}\right]$ be the interval during which there is no sensor data received at the controller. Then the value of $\varepsilon_{p,k}$ depends on the following three factors: the event-trigger error, network-induced delays and packet losses. This can be explained with the following simplified example.

Suppose the event is triggered at $k_l = 0$ and the controller received the event with no delay. The next event is triggered at $k = 3$ however the packet containing this event is lost. Then the event will be triggered again at $k = 4$ since the control input has not been changed and the trigger error keeps increasing. Suppose that the network-induced delay is $\tau = 2T_s$, then the time that the controller receives the event will be $k = 6$. Therefore, in this case we have $\varepsilon_{p,k} = 6T_s$. The following theorem gives the maximum timespan $\varepsilon_{p,k}$ that the physical system can tolerate.

Theorem 6 (Maximum Delay and Packet Loss): Consider the closed-loop system (64) without physical attacks and the control input is given by (75). Suppose the QFE estimator vector is updated by using (77) at the event-sampled instants and (79) during the inter-sampling period.

Theorem 7: Assume the communication network is under attacks such that the timespan $\varepsilon_{p,k}$ is always greater than ε_m. Then the physical system becomes unstable if ε_m satisfies

$$\begin{aligned} &\lambda_{\min}\{\Gamma\} \underset{\tau,\gamma}{E}\left\{\left\| A_p^{\varepsilon_m} x_{p,k_l} + \sum_{i=k_l}^{k_l+\varepsilon_m-1} A_p^{k_l+\varepsilon_m-i-1} B_p u_{p,i} \right\|^2\right\} \\ &\geq \lambda_{\max}\{\Gamma\} \underset{\tau,\gamma}{E}\left\{\left\| x_{p,k_l} \right\|^2\right\} + \kappa_{\min} \underset{\tau,\gamma}{E}\left\{\left\| \tilde{\Theta}_{k_l} \right\|^2\right\} \end{aligned}. \tag{84}$$

Proof: Let the last event triggered time be k_l. Then if the timespan $\varepsilon_{p,k}$ is always greater than ε_m, there will be no control updates during the interval $(k_l, k_l+\varepsilon_m)$. Select the Lyapunov function as

$$L_{p1,k} = L_{\Theta}\left(k_l^j\right) + L_{x_p}(k), \tag{85}$$

where $L_{\Theta,k} \triangleq \underset{\tau,\gamma}{E}\left\{\tilde{\Theta}^T_{k_l^j}\Omega^{-1}_{k_{l-1}^j}\tilde{\Theta}_{k_l^j}\right\}$ and $L_{x_p}(k) \triangleq \underset{\tau,\gamma}{E}\left\{x^T_{p,k}\Gamma x_{p,k}\right\}$. Then by using the error dynamics (79), one can get the first difference of $L_{\Theta,k}$, which is given by

$$\Delta L_{\Theta,k} = -\underset{\tau,\gamma}{E}\left\{\frac{\tilde{\Theta}^T_{k_{l-1}^{j-1}}Z^T_{k_{l-1}^{j-1}}Z_{k_{l-1}^{j-1}}\tilde{\Theta}_{k_{l-1}^{j-1}}}{1+Z^T_{k_{l-1}^{j-1}}\Omega_{k_{l-2}^{j-2}}Z_{k_{l-1}^{j-1}}}\right\}. \tag{86}$$

Since the regression vector satisfies the persistently exciting (PE) condition

$$0 < \underset{\tau,\gamma}{E}\left\{\frac{Z_{k_{l-1}^{j-1}}Z^T_{k_{l-1}^{j-1}}}{1+Z^T_{k_{l-1}^{j-1}}\Omega_{k_{l-2}^{j-2}}Z_{k_{l-1}^{j-1}}}\right\} \le 1, \tag{87}$$

we then have

$$\Delta L_{\Theta}\left(k_l\right) \le -\kappa_{\min}\underset{\tau,\gamma}{E}\left\{\left\|\tilde{\Theta}_{k_{l-1}}\right\|^2\right\}. \tag{88}$$

Furthermore, the first difference of $L_{x_p}(k)$ is given by

$$\begin{aligned}\Delta L_{x_p}(k) &= \underset{\tau,\gamma}{E}\left\{x^T_{p,k_l+\varepsilon_m}\Gamma x_{p,k_l+\varepsilon_m} - x^T_{p,k_l}\Gamma x_{p,k_l}\right\}\\ &\ge \lambda_{\min}\{\Gamma\}\left\|x_{p,k_l+\varepsilon_m}\right\|^2 - \lambda_{\max}\{\Gamma\}\left\|x_{p,k_l}\right\|^2.\end{aligned} \tag{89}$$

Therefore if the event is not triggered for enough long time, the difference of the second term in the Lyapunov function, $\Delta L_{x_p}(k)$, will keep increasing and become the dominant one in (85) and thus $\Delta L_{p,k}$. To be specific, if (84) is satisfied, by combining (88) and (89) we have

$$\begin{aligned}\Delta L_{p1,k} &= \Delta L_{\Theta}\left(k_l^j\right) + \Delta L_{x_p}\left(k\right) \\ &\geq \lambda_{\min}\left\{\Gamma\right\}\left\|x_{p,k_l+\varepsilon_m}\right\|^2 - \lambda_{\max}\left\{\Gamma\right\}\left\|x_{p,k_l}\right\|^2 + \Delta L_{\Theta}\left(k_l^j\right) \\ &\geq \kappa_{\min}\underset{\tau,\gamma}{E}\left\{\left\|\tilde{\Theta}_{k_l}\right\|^2\right\} + \Delta L_{\Theta}\left(k_l^j\right) \geq 0.\end{aligned}$$

Hence the stability of the physical system cannot be guaranteed if $\varepsilon_{p,k} \geq \varepsilon_m$ always holds.

Remark 5: Theorem 6 gives the maximum network delay and packet losses that the physical system can tolerate. Appropriate network defense must be launched once $\varepsilon_{p,k}$ exceeds this threshold, or the physical system needs to be shut down to prevent further damages.

5.2. ATTACK DETECTION FOR THE PHYSICAL SYSTEM

It is shown in the previous section that in the absence of attacks on the networks and the physical system, the system is asymptotically stable. If the network is under attacks such that (84) is satisfied, the physical system then becomes unstable. In this section, we examine the scenario where the network is in the healthy condition whereas the physical system suffers from attacks. To be specific, the detectability condition is derived under which the attacks on the physical system can be detected.

Consider the system described by (64) in the presence of physical attacks. Suppose that the attack input $w_{p,k}$ is considered as a disturbance and no defenses will be launched, if it is smaller than a given threshold, i.e., $\left\|w_{p,k}\right\| \leq w_{p,M}$. Then the following theorem shows the boundedness of the system state vector for the case that $\left\|w_{p,k}\right\| \leq w_{p,M}$.

Theorem 8 (Physical Attack Detection): Consider the closed-loop system (64) in the absence of attacks on the network and let the control input be given by (75) with u_0 being

an initial admissible control input. Suppose the QFE estimator vector is updated by using (77) at the event-sampled instants and (79) during the inter-sampling period. Select the event-trigger condition given by (83). Assume the regression vector $\xi_{k_l}^j$ satisfies the PE condition. Let $w_{p,M}$ be the threshold below which the attack input $w_{p,M}$ is considered as a disturbance. Then the attack can be detected when the system states vector satisfies $\underset{\tau,\gamma}{E}\left\{\left\|x_{p,k_l}\right\|\right\} > \Upsilon_p$ where $\Upsilon_{p,k}$ is defined in the proof.

Proof: Consider the following Lyapunov function:

$$L_{p2,k} = \bar{\Pi} L_\Theta\left(k_l^j\right) + L_{x_p}\left(k_l\right), \tag{90}$$

where $L_\Theta\left(k_l^j\right)$ and $L_{x_p}\left(k_l\right)$ are defined in (85) and $\bar{\Pi} \triangleq \eta_1\eta_3\left\|\Omega_0\right\|$ with $\eta_1 > 1$ and η_3 defined later in the proof. First, we consider case at the aperiodic event-sampled instants. Substitute the system dynamics (64) into $L_{x_p}\left(k\right)$ and one can get the first difference of $L_{x_p}\left(k_l\right)$, which is given by

$$\begin{aligned}
&\Delta L_{x_p}\left(k_l\right) = \underset{\tau,\gamma}{E}\left\{x_{p,k_l}^T \Gamma x_{p,k_l} - x_{p,k_l-1}^T \Gamma x_{p,k_l-1}\right\} = \\
&\underset{\tau,\gamma}{E}\left\{\begin{matrix}\left(A_p x_{p,k_l-1} + B_p u_{p,k_l-1} + W_p w_{p,k_l-1}\right)^T \Gamma\left(A_p x_{p,k_l-1} + B_p u_{p,k_l-1} + W_p w_{p,k_l-1}\right) \\ -x_{p,k_l-1}^T \Gamma x_{p,k_l-1}\end{matrix}\right\}.
\end{aligned} \tag{91}$$

Applying C-S inequality yields

$$\begin{aligned}
&\Delta L_{x_p}\left(k_l\right) \le \\
&\underset{\tau,\gamma}{E}\left\{2\left(A_p x_{p,k_l-1} + B_p u_{p,k_l-1}\right)^T \Gamma\left(A_p x_{p,k_l-1} + B_p u_{p,k_l-1}\right) + 2w_{p,k_l-1}^T \breve{W}_p w_{p,k_l-1} - x_{p,k_l-1}^T \Gamma x_{p,k_l-1}\right\}
\end{aligned}$$

$$= \underset{\tau,\gamma}{E}\left\{\begin{matrix}x_{p,k_l-1}^T \bar{\Gamma} x_{p,k_l-1} + 4x_{p,k_l-1}^T\left(B_p \tilde{K}_{p,k_l-1}\right)^T \Gamma A_p x_{p,k_l-1} \\ +2x_{p,k_l-1}^T\left(B_p \tilde{K}_{p,k_l-1}\right)^T \Gamma + 2w_{p,k_l-1}^T \breve{W}_p w_{p,k_l-1}\end{matrix}\right\}$$

$$\leq \underset{\tau,\gamma}{E}\left\{\begin{array}{l} -\lambda_{\min}\left\{\bar{\Gamma}\right\}\left\|x_{p,k_l-1}\right\|^2+4\left\|x_{p,k_l-1}^T\left(B_p\tilde{K}_{p,k_l-1}\right)^T\Gamma\right\|\times \\ \left\|A_p x_{p,k_l-1}\right\|+2\|\Gamma\|\left\|B_p\tilde{K}_{p,k_l-1}x_{p,k_l-1}\right\|+2w_{p,k_l-1}^T\breve{W}_p w_{p,k_l-1} \end{array}\right\}, \tag{92}$$

where $\bar{\Gamma}\triangleq 2A_p^T\Gamma A_p-\Gamma$ and $\breve{W}_p\triangleq W_p^T\Gamma W_p$.

Applying Young's inequality, we have

$$\Delta L_{x_p}\left(k_l\right)\leq \underset{\tau,\gamma}{E}\left\{\begin{array}{l} -\lambda_{\min}\left\{\bar{\Gamma}\right\}\left\|x_{p,k_l-1}\right\|^2+2\left\|\varepsilon_1 A_p x_{p,k_l-1}\right\|^2+ \\ 2\left\|\left(\Gamma+\dfrac{\Gamma^2}{\varepsilon_1}\right)B_{p,M}\tilde{u}_{p,k_l-1}\right\|^2+2\lambda_{\max}\left\{\breve{W}_p\right\}w_{p,M}^2 \end{array}\right\}, \tag{93}$$

where ε_1 is a positive constant and $B_{p,M}$ is the bound of B_p.

Since the estimation error of the control input, $\tilde{u}_{p,k_l-1}$, satisfies [14]

$$\underset{\tau,\gamma}{E}\left\{\left\|\tilde{u}_{p,k_l-1}\right\|^2\right\}\leq \underset{\tau,\gamma}{E}\left\{\begin{array}{l} \left(4G_{p,M}\left\|R_{p,k_l}^{-1}\right\|^2+2\varepsilon_2\right)\left\|x_{p,k_l-1}\right\|^2+ \\ \left(\left\|R_{p,k_l}^{-1}\right\|^2+\dfrac{2G_{p,M}^2\left\|R_{p,k_l}^{-1}\right\|^4}{\varepsilon_2}\right)\left\|\tilde{\Theta}_{k_l-1}\right\|^2\left\|x_{p,k_l-1}\right\|^2 \end{array}\right\}, \tag{94}$$

where $G_{p,M}$ is the bound of $G_{p,k}^{ux}$ and ε_2 is a positive constant.

Substituting (94) into (93) yields

$$\begin{array}{l} \underset{\tau,\gamma}{E}\left\{\Delta L_{x_p}\left(k_l\right)\right\}\leq -\left(\lambda_{\min}\left\{\bar{\Gamma}\right\}-\eta_2\right)\underset{\tau,\gamma}{E}\left\{\left\|x_{p,k_l-1}\right\|^2\right\} \\ +\eta_3\|\Gamma\|\underset{\tau,\gamma}{E}\left\{\left\|\tilde{\Theta}_{k_l-1}\right\|^2\left\|x_{p,k_l-1}\right\|^2+2\lambda_{\max}\left\{\breve{W}_p\right\}w_{p,M}^2\right\}, \end{array} \tag{95}$$

where $\eta_2\triangleq 2\left\|\left(\Gamma+\dfrac{\Gamma^2}{\varepsilon_1}\right)B_{p,M}\right\|^2\left(4G_{p,M}\left\|R_{p,k_l}^{-1}\right\|^2+2\varepsilon_2\right)+\left\|\varepsilon_1 A_p\right\|^2$ and

$$\eta_3\triangleq 2\|\Gamma\|\left\|\left(1+\frac{\Gamma}{\varepsilon_1}\right)B_{p,M}\right\|^2\left(\left\|R_{p,k_l}^{-1}\right\|^2+\frac{2G_{p,M}^2\left\|R_{p,k_l}^{-1}\right\|^4}{\varepsilon_2}\right).$$

Combining (88) and (95), we have the total first difference of the Lyapunov function, which is given by

$$\begin{aligned}\Delta L_{p2,k} \le & -\left(\lambda_{\min}\left\{\bar{\Gamma}\right\}-\eta_2\right)\underset{\tau,\gamma}{E}\left\{\left\|x_{p,k_l-1}\right\|^2\right\} \\ & -\left(\bar{\Pi}-\left\|\Omega_0\right\|\eta_3\right)\kappa_{\min}\underset{\tau,\gamma}{E}\left\{\left\|\tilde{\Theta}_{k_l-1}\right\|^2\right\}+2\lambda_{\max}\left\{\breve{W}_p\right\}w_{p,M}^2 .\end{aligned} \tag{96}$$

Therefore, the first term in (96) is negative by selecting the appropriate $\lambda_{\min}\left\{\bar{\Gamma}\right\}$. Recalling the definition of $\bar{\Pi}$ in the beginning of the proof, one can conclude that the second term is also negative.

For the interval between two event-sampled instants, we have $\Delta L_{p2,k}<0$ because the trigger condition (83) guarantees $L_{x_p}\left(k_l\right)<0$ while (88) guarantees $L_{\Theta}\left(k_l^j\right)<0$. Combining these two cases, we conclude that in the presence of physical attacks bounded by $\left\|w_{p,k}\right\|\le w_{p,M}$, the system state vector is bounded in the mean by

$$\underset{\tau,\gamma}{E}\left\{\left\|x_{p,k_l-1}\right\|\right\}\le\sqrt{\frac{2\lambda_{\max}\left\{\breve{W}_p\right\}}{\left(\lambda_{\min}\left\{\bar{\Gamma}\right\}-\eta_2\right)}}w_{p,M}\triangleq\Upsilon_p . \tag{97}$$

That is to say, if the state vector satisfies $\underset{\tau,\gamma}{E}\left\{\left\|x_{p,k_l}\right\|\right\}>\Upsilon_p$, it implies that the attack input exceeds the threshold (i.e., $\left\|w_{p,k}\right\|>w_{p,M}$), thus is considered as an attack.

6. SIMULATION AND HARDWARE IMPLEMENTATION RESULTS

In order to show the effectiveness of the proposed attack detection scheme, several scenarios involving both the networks and physical systems are considered in the simulation.

6.1. NETWORK SIMULATION RESULTS

On the network side, the first scenario is the simulation for the healthy case where there is no attack. In the second scenarios, we pick the jamming attack introduced in the previous section as an example to show the attack detection and estimation results.

The simulation is performed in MATLAB with the following parameters for the communication networks: sampling period $T = 100\text{ms}$, total simulation time $T_s = 500T$, standard transmission rate $\upsilon_0 = 300$ packets per T,the desired flow in the bottleneck node $\rho_0 = 300$ packets, $m = 3, l_1 = 1/8, l_1 = 1/4$, $l_1 = 1/2$, P_k and R_k are identity matrices with appropriate dimensions.

6.1.1. Scenario A1 (Normal Case). Figure 6.1 shows that in the absence of attacks, the QFE error becomes very close to zero, which verifies the result given in Theorem 1. Moreover, Figure 6.2 shows the actual and desired number of packets in the bottleneck node and the actual number of packets fluctuates around the desired value, which agrees with the conclusions of Theorem 2.

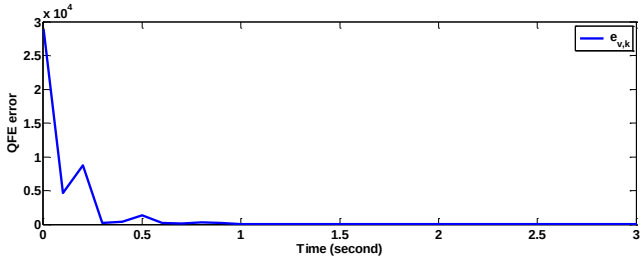


Figure 6.1. QFE error converges in the absence of attacks.

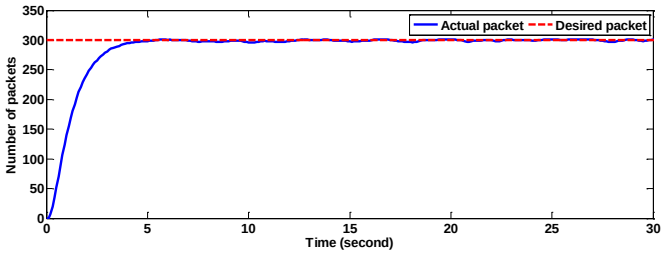


Figure 6.2. Actual and desired number of packets in the bottleneck node.

6.1.2. Scenario A2 (Under Attack). In this scenario, the jamming attack is introduced at $t = 250T_s$. As depicted in Figure 6.2, the attacker is assumed to increase the number of jammers in the network linearly along with the time until to the maximum value. As a result, the packets injected by the attacker will increase to the maximum of 500 packets per sampling period. The estimation error of the flow, plotted in Figure 6.3, exceeds the threshold shortly after the attack is launched and thus it can be detected, which confirms Theorem 3.

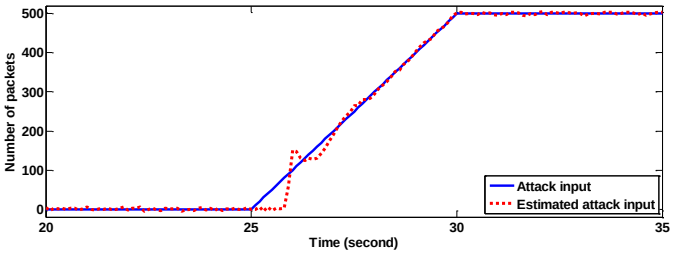


Figure 6.3. Injected flow by the jamming attack with estimation.

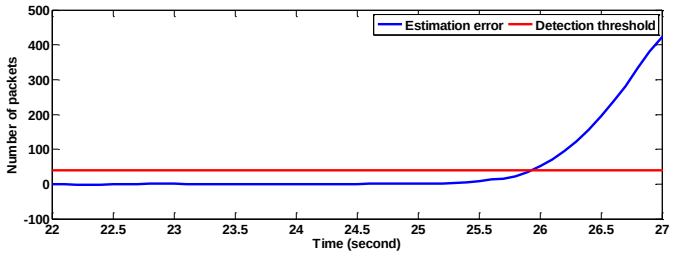


Figure 6.4. Estimation error exceeds the threshold in Scenario A2.

Upon detection, if the observer introduced in Theorem 4 is applied, then the attack flow can be estimated. As shown in Figure 6.2, the estimated attack input given by the observer is able to track the actual attack input after only a few seconds. With the estimated attack flow, one can estimate the delay and packet losses in the link, which can be further utilized to tune the controller parameters of the physical systems.

6.2. SIMULATION RESULTS FOR THE PHYSICAL SYSTEMS

On the side of the physical plant, we first evaluate the performance of the hybrid event-sampled controller in the absence of physical and network attacks. Then we show that the system becomes unstable when the delays and packet losses exceed a certain threshold due to attacks on the network. Finally we demonstrate that the proposed detection scheme is able to detect the attacks on the physical system.

The inverted pendulum system is considered in the simulation of the physical system. The continuous system dynamics are given by

$$\dot{x}(t) = \begin{bmatrix} 0 & 1 \\ \frac{g}{l} - \frac{k}{ml^2} & 0 \end{bmatrix} x(t) + \begin{bmatrix} 0 \\ \frac{1}{ml^2} \end{bmatrix} u(t) \tag{98}$$

with $l = 2$, $g = 10$, $m = 1$ and $k = 5$. The system is discretized with the sampling period $T_{p,s} = 100ms$. The penalty matrices $P_{p,k}$ and $R_{p,k}$ are identity matrices with appropriate dimensions. The system state is initialized with $x_0 = [2, -3]$ and the total simulation time is 500 seconds.

6.2.1. Scenario B1 (Normal Case). In this scenario, the network in assumed be in the healthy condition. To be specific, the maximum delay is 150ms and the packet loss rate is 0.1, as shown in Figure 6.5.

As shown in Figure 6.6, the system states converge to close to zero after about eight seconds, although the initial states are fairly far from their target values. Figure 6.7 shows the comparison of the evolution of the parameter estimation error between a traditional time-driven Q-learning and the hybrid event-triggered learning approach.

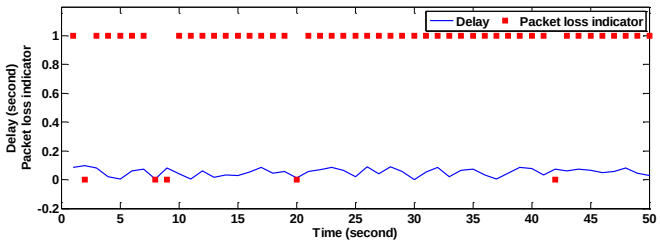


Figure 6.5. Delay and packet loss in Scenario B1.

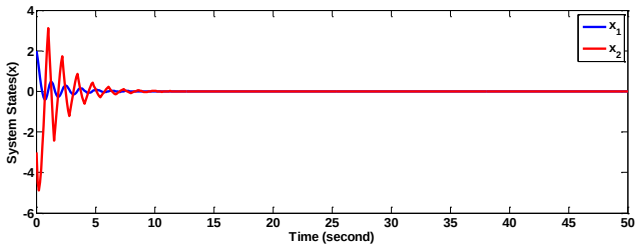


Figure 6.6. Convergence of system states in Scenario B1.

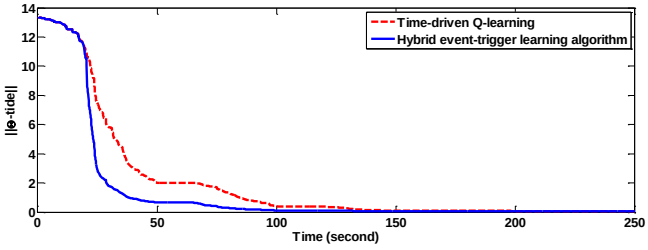


Figure 6.7. Estimation error comparison between the time-driven Q-learning and the hybrid event-trigger learning algorithm.

It can be observed that the convergence time for the hybrid learning algorithm is much faster than the time-driven approach. Therefore, Figure 6.6 and Figure 6.7 confirm Theorem 5.

6.2.2. Scenario B2 (Network under Attack). In this scenario, we suppose the network is under attack such that the maximum delay is 250ms and the packet loss rate is 0.2, as shown in Figure 6.8. As a result, the overall delay exceeds the maximum value that the system can tolerate. Therefore, as depicted in Figure 6.9, the physical system becomes unstable, which confirms Theorem 6.

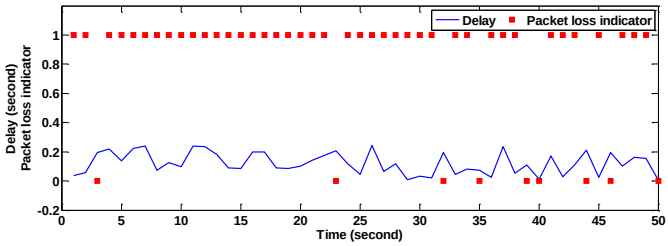


Figure 6.8. Delay and packet loss in Scenario B2.

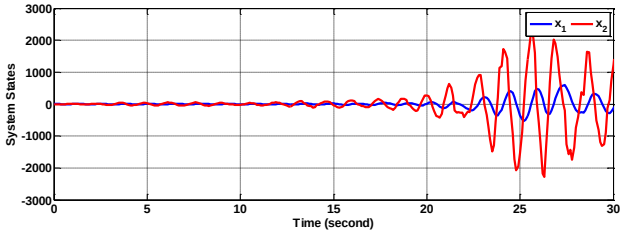


Figure 6.9. System becomes unstable in Scenario B2.

6.2.3. Scenario B3 (Physical System under Attack). In this scenario, we first introduce an actuator attack on the physical system at $t_a = 250T_{p,s}$ where the input is manipulated from $u_{p,k}$ to $u_{p,k} + \Delta u_{p,k}$ with $\Delta u_{p,k} = 1.2(k - 250)$ as shown in Figure 6.10.

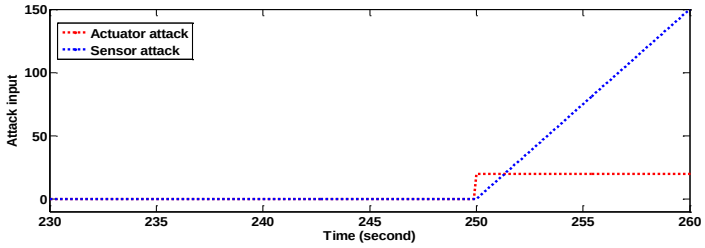


Figure 6.10. Attack on the physical system in Scenario B3.

As a result, the magnitude of the states increases after the launch of the attack and exceeds the detection threshold shortly, as shown in Figure 6.11.

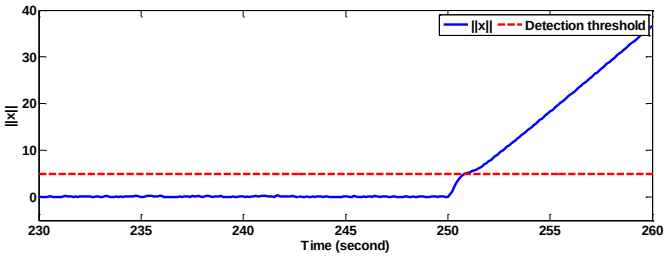


Figure 6.11. Actuator attack detection for the physical system.

Next, a sensor attack is introduced where the measured state is manipulated from $x_{p,k}$ to $x_{p,k} + \Delta x_{p,k}$ with $\Delta x_{p,k} = \begin{bmatrix} 20 & 20 \end{bmatrix}^T$, as shown in Figure 6.10. Figure 6.12 shows the detection results, where it can be seen that right after the attack is launched, the magnitude of the states exceeds the threshold. Therefore, the attack can be detected, which verifies the conclusion of Theorem 7.

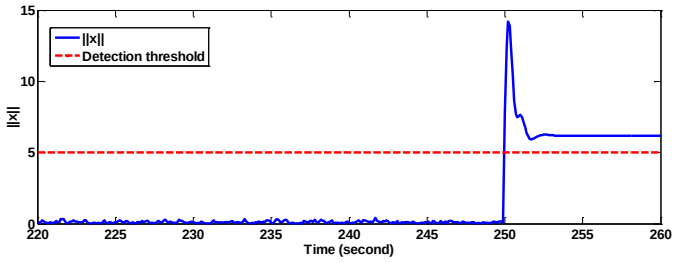


Figure 6.12. Actuator attack detection for the physical system.

7. CONCLUSIONS AND FUTURE WORK

Many cyber-attacks on the networked control systems target at the availability rather than the secrecy of the data. For such attacks, even the most complicated encryption algorithm cannot defend them. To address this issue, in this paper, we proposes a novel cyber-attack detection scheme that is capable of capturing the vulnerable communication links, which is challenging because the system dynamics are unknown. The detection of the attacks is faster than the traditional approach where one has to wait for the physical states to be deteriorated. The proposed detection scheme for the physical system is able to detect both sensor and actuator attacks. Moreover, the knowledge of the maximum delays and packet losses that the system can tolerate helps the operator protect the plant from further damages based on the ongoing network condition. The limitation of proposed scheme is that it is applicable only to those network attacks causing delays and packets losses.

8. REFERENCES

[1] P. Lee, A. Clark, L. Bushnell, and R. Poovendran, "A passivity framework for modeling and mitigating wormhole attacks on networked control systems," Automatic Control, IEEE Transactions on 59, no. 12, pp. 3224-3237, 2014.

[2] Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of jamming attacks in time-critical wireless applications," Mobile Computing, IEEE Transactions on 13, no. 8, pp. 1746-1759, 2014.

[3] M, Zhu, and S. Martinez, "On the performance analysis of resilient networked control systems under replay attacks," Automatic Control, IEEE Transactions on 59, no. 3, pp. 804-808, 2014.

[4] N. Falliere, L. O. Murchu, and E. Chien, W32.Stuxnet Dossier Symantec Corporation, 2011.

[5] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," Automatica, vol. 51, pp. 135-148, 2015.

[6] H. Sandberg, S. Amin, and K. H. Johansson, "Cyber-physical security in networked control systems: an introduction to the issue," IEEE Control Systems, vol. 35, no. 1, pp. 20-23, 2015.

[7] M. Mozaffari-Kermani, K. Tian, R. Azarderakhsh, and S. Bayat-Sarmadi, "Fault-resilient lightweight cryptographic block ciphers for secure embedded systems," Embedded Systems Letters, IEEE 6, no. 4, pp. 89-92, 2014.

[8] D. Browning, "Flow control in high-speed communication networks," Communications, IEEE Transactions on 42, no. 7 pp. 2480-2489, 1994.

[9] C. Li, and E. Modiano, "Receiver-based flow control for networks in overload," Networking, IEEE/ACM Transactions on 23, no. 2, pp. 616-630, 2015.

[10] J. Jin, W. Wang, and M. Palaniswami, "A simple framework of utility max-min flow control using sliding mode approach," Communications Letters, IEEE 13, no. 5, pp. 360-362, 2009.

[11] P. Huang, X. Lin, and C. Wang, "A low-complexity congestion control and scheduling algorithm for multihop wireless networks with order-optimal per-flow delay," IEEE/ACM Transactions on Networking (TON) 21, no. 2, pp. 495-508, 2013.

[12] H. Xu , S. Jagannathan, and F.L. Lewis, "Stochastic optimal control of unknown linear networked control system in the presence of random delays and packet losses," Automatica 48, no. 6, pp. 1017-1030, 2012.

[13] A. Sahoo, H. Xu, and S. Jagannathan, "Adaptive neural network-based event-triggered control of single-input single-output nonlinear discrete-time systems," IEEE Transactions on Neural Networks and Learning Systems, vol. 27, no. 1, 2016.

[14] V. Narayanan and S. Jagannathan, "Distributed adaptive optimal regulation of uncertain large-scale interconnected systems using hybrid q-learning approach," IET Control Theory & Applications, 2016.

[15] Y. Chen, S. Kar, and J. Moura, "Cyber-physical systems: Dynamic sensor attacks and strong observability," In Acoustics, Speech and Signal Processing (ICASSP), IEEE International Conference on, pp. 1752-1756, April 2015.

[16] G. Tao, S. Chen, X. Tang, and S.M. Joshi, Adaptive Control of Systems with Actuator Failures, Springer Science & Business Media, 2013.

[17] J. C. Bolot, "End-to-end packet delay and loss behavior in the Internet," In ACM SIGCOMM Computer Communication Review, vol. 23, no. 4, pp. 289-298, 1993.

[18] Y. T. Hou, S. S. Panwar, and H. Tzeng, "On generalized max-min rate allocation and distributed convergence algorithm for packet networks," Parallel and Distributed Systems, IEEE Transactions on 15, no. 5, pp. 401-416, 2014.

[19] E. Altman, and T. Basar, "Optimal rate control for high speed telecommunication networks," In Decision and Control, Proceedings of the 34th IEEE Conference on, vol. 2, pp. 1389-1394, December 1995.

[20] J. Luo, X. Yang, J. Wang, J. Xu, J. Sun, and K. Long, "On a mathematical model for low-rate shrew DDoS," Information Forensics and Security, IEEE Transactions on 9, no. 7, pp. 1069-1083, 2014.

[21] P. Tague, D. Slater, R. Poovendran, and G. Noubir, "Linear programming models for jamming attacks on network traffic flows," In Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops, IEEE 6th International Symposium on, pp. 207-216, April 2008.

[22] Y. Ge, Q. Chen, M. Jiang, and Y. Huang, "Modeling of random delays in networked control systems," Journal of Control Science and Engineering, vol. 2013, Article ID 383415, 9 pages, 2013.

[23] W. Zhang, and J. He, "Statistical modeling and correlation analysis of end-to-end delay in wide area networks," Software Engineering, Artificial Intelligence, Networking, and Parallel/ Distributed Computing, IEEE Eighth ACIS International Conference on 3, pp. 968-973, 2007.

[24] I. Cerutti, A. Fumagalli, and P. Gupta, "Delay models of single-source single-relay cooperative ARQ protocols in slotted radio networks with Poisson frame arrivals," IEEE/ACM Transactions on Networking (TON) 16, no. 2, pp. 371-382, 2008.

[25] K. Han, S. Kim, Y. Kim, and J. Kim, "Internet control architecture for internet-based personal robot," Autonomous robots 10, no. 2, pp. 135-147, 2001.

[26] S. Keshav, "A control-theoretic approach to flow control," ACM, vol. 21, no. 4, pp. 3-15, 1991.

[27] S. Jagannathan, Neural Network Control of Nonlinear Discrete-time Systems, CRC Press, Boca Raton, RL, 2006.

[28] F.L. Lewis and V.L. Syrmos, Optimal Control, 2nd. Wiley, New York, 1995.

[29] K.S., Narendra, and S. Mukhopadhyay, "To communicate or not to communicate: a decision-theoretic approach to decentralized adaptive control," Proceeding of American Control Conference (ACC), pp. 6369-6376, July 2010.

[30] M. Bishop, Computer Security: Art and Science, vol. 200. Addison-Wesley, 2012.

[31] P. Tague, D. Slater, R. Poovendran, and G. Noubir, "Linear programming models for jamming attacks on network traffic flows," In Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops, IEEE 6th International Symposium on, pp. 207-216, May 2008.

[32] P. Raj, and P. B. Swadas, "Dpraodv: A dyanamic learning system against blackhole attack in AODV based manet," arXiv preprint: 0909.2371, 2009.

[33] A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants," In Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communications, pp. 75-86. ACM, August 2003.

[34] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," Automatic Control, IEEE Transactions on 58, no. 11, pp. 2715-2729, 2013.

[35] K. S. Narendra and A. M., ANnaswamy, Stable Adaptive Systems, New York, NY, USA: Dover, 2015.

V. ATTACK DETECTION AND APPROXIMATION IN NONLINEAR NETWORKED CONTROL SYSTEMS USING NEURAL NETWORKS

Haifeng Niu and S. Jagannathan

In networked control systems, the communication links, sensors and actuators are vulnerable to a variety of potential malicious attacks. Certain class of attacks on the communication network is known to raise traffic flows causing delays and packet losses to increase. In this paper, we propose a novel attack detection and estimation scheme that is capable of capturing the abnormal traffic flow as a result of a class of attacks on the communication links within the feedback loop of a control system. The network flow at the bottleneck node is modeled as a nonlinear system with unknown dynamics. By using an observer, network attack detection residual is generated which in turn is utilized to determine the onset of an attack in the communication network when the residual exceeds a predefined threshold. For the physical system, we develop an attack detection scheme by using an optimal or approximate dynamic programming-based event-triggered controller in the presence of network delays and packet losses. Moreover, attacks on the sensor or actuators of the physical system can be detected and further estimated with the proposed attack detection scheme.

1. INTRODUCTION

Networked Control Systems (NCS) are feedback systems with control loops closed by using a communication network [1]. In NCS, the digital controllers receive measured data from sensors and transmit control commands to the actuators through a communication network. This communication network is vulnerable to adversaries due to two reasons [2]: 1) the components are resource-constrained and low-cost embedded devices and it is difficult to deploy advanced security algorithms; and 2) in a few applications such as smart grid, the networks are distributed geographically.

The defense methodology, therefore, for NCS has received significant attention. A vast literature focusing on the development of light-weight encryption methods was summarized in [3][4]. However, unlike the traditional information technology (IT) systems, the protection of data confidentiality and integrity alone is far from enough in NCS because the physical system can be affected by the network attacks through the feedback actuation. One example is that the network delay induced by jamming attacks could lead to control system performance degradation which may potentially lead to instability [5].

Besides encryption methods, there is also significant effort aiming at protecting the information security of the networks, but from a different perspective [6-8]. For instance, in [1], the denial of service (DoS) flooding attacks by a continuous-time Markov chain to compute security measures is introduced using state space approach. The authors in [7] study the cyber defense by modeling the actions of the attacker and the defender as a stochastic zero-sum game. A similar game-theoretic approach has been adopted in [8]

where the authors generate expected probabilities of the attacks and build a transition model to access the network security.

In [3-8], the communication network security is considered whereas others [9-12] concentrate on the detection of state abnormality in the physical system due to attacks on the network, sensor and actuator devices. For instance, the authors in [9] study attacks on control system components compromising of measurement and actuator data integrity and availability, and model their effect on the physical system dynamics. In [10], the state of the physical system under false data injection attack is represented with an additive term. In [11], the estimation and control of linear systems when sensors or actuators are corrupted by an attack is provided, together with a secure local control loop that can improve the resilience of the system. The authors in [12] analyze the stealthy attacks and propose methods to approximate the reachable set of states for such stealthy adversaries.

However, these research efforts [9-12] assume the system dynamics to be linear and known whereas in real application they may become uncertain under network conditions [5]. Although this issue has been addressed in [5][13] with Q-learning and zero-sum game theoretic formulation, there is another major concern that has not been covered yet. To be specific, the communications networks are probably already compromised when a significant deviation is observed in the physical system state vector. For this reason, it is crucial to monitor not only the state vector of the physical system, but also the condition in the communication links. Therefore, in this paper, we propose a detection scheme that is capable of capturing the abnormal traffic flow in the communication links for certain class of cyber-attacks.

Flow control has been studied in the literature [2][20-22]. For example, authors in [20] use a Kalman state estimator in discrete-time for reactive flow control in networks that do not reserve bandwidth. An optimal rate-based flow controllers is derived in [21] by using the decentralized Linear Quadratic Gaussian theory. The authors in [22] proposed a distributed algorithm using a feedback-based flow control mechanism which converges to the generalized max-min rate allocation.

However, to the best of our knowledge, minimal effort has been spent on studying the flow control from the perspective of network security when the network is attacked by injecting traffic flow. In particular, the authors in [2] present a control-theoretic framework for modeling and analyzing defense against the jamming attacks on cyber-physical systems. However, the assumption that the system representation is linear and known in [2][20][21], which may not be realistic since physical systems are invariably nonlinear.

In this paper, we begin by introducing the nonlinear representation of the traffic flow under cyber-attacks for the communication network. Next, we derive the neural network (NN)-based controller that stabilizes the flow within a desired level during healthy conditions and without attacks. By using an adaptive observer, network attack detection residual is generated which in turn is utilized to determine the onset of an attack in the communication network when the residual exceeds a predefined threshold. Then we give the detectability condition which is a mathematical inequality that determines whether an attack is detectable or not.

Next, the performance of the attack detection scheme is discussed. Upon detecting attacks, a novel observer is proposed in order to estimate the flow that has been injected by the malicious attacker. For the physical system, we introduce an event-triggered control

scheme in the presence of network delays and packet losses resulting of network attacks. Moreover, attacks on the sensor or actuator of the physical system can be detected and further estimated with the proposed attack detection scheme.

The contributions of the paper include: 1) the development of novel observer-based network attack detection and estimation scheme along with detectability condition for nonlinear NCS with unknown system dynamics; 2) demonstration of the proposed scheme in the presence of a class of attacks with specific adversary models; 3) development of event-triggered controller in the presence of network delays and packet losses and physical attacks on the sensor and the actuator; and 4) the development of the attack detection and estimation for attacks on the physical system.

The rest of this paper is organized as follows. In Section 2, we introduce the nonlinear flow model under cyber-attacks, followed by the observer and controller design. The observer-based network attack detection and estimation scheme along with detectability condition for the networks is presented in Section 3. The event-trigger control scheme, the attack detection and estimation for the physical system are presented in Section 4. The simulation results and analysis are given in Section 5 and conclusions in Section 6.

2. CONTROLLER AND OBSERVER DESIGN FOR THE NONLINEAR FLOW MODEL

2.1. NONLINEAR FLOW MODEL

In this section, first the communication network in a NCS is modeled and a nonlinear flow controller is designed. Figure 2.1 shows the block diagram of a NCS, where both the controller commands and the sensor data are transmitted through a wired or wireless communication link. In this section, we propose a nonlinear model in discrete-time for the traffic flow at the bottleneck link in the presence of attacks. It is verified both theoretically and experimentally [23] that the performance measures such as the delay and transmission rate are determined by the bottleneck node and therefore a mild assumption that is widely reported in the literature [24][25] is asserted.

The buffer length at the bottleneck node can be described by the following nonlinear discrete time mode:

$$\begin{aligned} x_{k+1} &= f(x_k) + Tu_k + d_k + w_k \\ y_k &= \begin{bmatrix} y_{1,k} \\ y_{2,k} \end{bmatrix} = \begin{bmatrix} h_1(x_k) \\ h_2(x_k) \end{bmatrix} \end{aligned} \quad , \tag{1}$$

where $x_k, u_k, d_k, w_k \in \mathbb{R}^n$ is the buffer length, input rate, disturbances, and attacker input at the bottleneck node at instant time k, respectively, T being the sampling interval, and nonlinear function $f(\cdot)$ represents the uncertain actual traffic accumulation and is a function of buffer length and service capacity. y_k is the system output where $y_{1,k}$ and $y_{2,k}$ stands for the delay and packet loss, respectively. The relationship between the delay (packet loss) and current buffer length is described by the stochastic function h_1 (h_2).

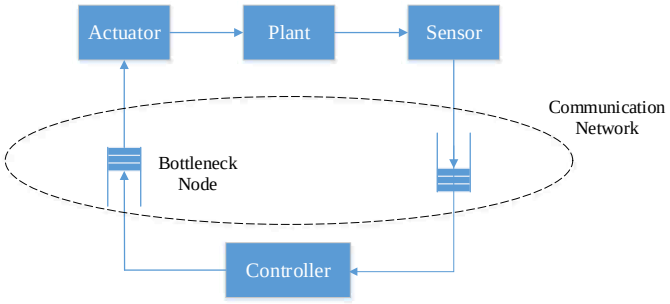


Figure 2.1. Diagram of a typical NCS.

Let the desired buffer length at instant time k be $x_{d,k}$ and define the tracking error of the buffer length as

$$e_k = x_k - x_{d,k}\,. \tag{2}$$

The objective is to derive the appropriate input flow rate u_k such that the difference between the desired and actual buffer length can be minimized. Substituting the system dynamics (2) into (1), we have the tracking error dynamics

$$e_{k+1} = f\left(x_k\right) + Tu_k + d_k + w_k - x_{d,k+1}\,. \tag{3}$$

Since the nonlinear function $f(\cdot)$ is unknown, a one-layer neural network (NN) will be utilized to estimate $f(\cdot)$. Let

$$f\left(x_k\right) = \theta^T \varphi\left(x_k\right) + \varepsilon_k\,, \tag{4}$$

where θ^T is a vector of constant weights bounded by $\|\theta\| \le \theta_M$ and $\varphi(\cdot)$ is the activation function bounded by $\varphi(\cdot) \le \varphi_M$. ε_k is the NN functional construction error vector. Define the output of the NN as

$$\hat{f}(x_k) = \hat{\theta}_k^T \varphi(x_k) . \tag{5}$$

Now define the input u_k as

$$u_k = \left(-\hat{f}(x_k) + x_{d,k+1} + Ke_k\right)/T , \tag{6}$$

where K is a diagonal feedback gain matrix. Substituting (6) back into (3) yields the closed-loop tracking error dynamics

$$e_{k+1} = Ke_k + \tilde{\theta}_k^T \varphi(x_k) + \varepsilon_k + d_k + w_k , \tag{7}$$

where $\tilde{\theta}_k^T = \theta^T - \hat{\theta}_k^T$ is the parameter error during the estimation. From (7) it can be seen that the tracking error in the buffer length is driven by the modeling parameter error as well as the disturbances and the attacker input.

Assumption 1: (1) The desired buffer length $x_{d,k}$ is bounded [26]. (2) The NN reconstruction error ε_k is bounded by ε_M , a known constant. [26]. (3) The disturbance and the attack flow are bounded by known constants d_M and w_M respectively. (4)Next, a controller design that stabilizes the buffer length to the desired level is revisited [26]. After that, we will present the proposed observer and show that the estimation error of the buffer length and the modeling parameter error converge to a small subset.

It has been reported in the literature [27] that the network state can be easily measured when the servers at the output queues are Rate Allocating Servers and the transport protocol supports the Packet-Pair probing technique. Therefore, in this paper, the network state described by input rate and the current buffer length in the link are considered accessible. Next, a nonlinear NN controller design that stabilizes the buffer length to the desired level is revisited [26]. After that, we will present the proposed observer and show

that the estimation error of the buffer length and the modeling parameter error converge to a small subset in the absence of attack input first and with attack input.

2.2. CONTROLLER DESIGN

First the following definition and Theorem 1 are needed before presenting the observer.

Definition 1: Consider the following nonlinear system

$$x_{k+1} = f(x_k, u_k) \tag{8}$$

where x_k and u_k is the state vector and input vector, respectively. The solution is said to be uniformly ultimately bounded (UUB) if for all $x_{k_0} = x_0$, there exist a $\mu \in \mathbb{R}^+$ and an $N(\mu, x_0) \in \mathbb{Z}^+$ such that $\|x_k\| \le \mu$ for all $k \ge k_0 + N$.

Theorem 1 [26]: Consider the flow model at the bottleneck node described by (1). Select the flow input rate (6) with the parameter update law provided by

$$\hat{\theta}_{k+1} = \hat{\theta}_k + \alpha\varphi(x_k) e_{k+1}^T - \Gamma \left\| I - \alpha\varphi(x_k)\varphi^T(x_k) \right\| \hat{\theta}_k , \tag{9}$$

where $\Gamma > 0$ is a design parameter. Then the tracking error of the buffer length e_k , and the modeling parameter error $\hat{\theta}_k$ are UUB, if the following conditions are satisfied:

$$\begin{array}{c} \alpha \left\| \varphi(x_k) \right\|^2 < 1 \\ 0 < \Gamma < 1 \\ K_M < 1/\sqrt{\bar{\sigma}} \end{array} , \tag{10}$$

where K_M is the maximum singular value of the gain matrix K and $\bar{\sigma}$ is given by

$$\bar{\sigma} = \frac{2\alpha\Gamma \left\| \varphi(x_k) \right\|^2 \left(1 - \alpha \left\| \varphi(x_k) \right\|^2\right) + 1}{1 - \alpha \left\| \varphi(x_k) \right\|^2} + \Gamma^2 \left(1 - \alpha \left\| \varphi(x_k) \right\|^2\right). \tag{11}$$

Next the observer is introduced to generate the estimated buffer length even though it is measured. The purpose of the observer is to generate the attack detection residual.

2.3. OBSERVER DESIGN

Let $\hat{x}_k$ be the estimated buffer length and the observer is described as

$$\hat{x}_{k+1} = \hat{\theta}_k^T \varphi(x_k) + Tu_k - L(x_k - \hat{x}_k), \tag{12}$$

where $L \in \mathbb{R}$ is the observer feedback gain matrix. Define the estimation error as $\tilde{x}_k = x_k - \hat{x}_k$. Combing (12) and (1) yields the estimation error dynamics

$$\tilde{x}_{k+1} = L\tilde{x}_k + \tilde{\theta}_k^T \varphi(x_k) + \varepsilon_k + d_k + w_k. \tag{13}$$

Theorem 2: Consider the flow model at the bottleneck node described by (1) and the observer described by (12). Select the flow input rate (6) with the parameter update law provided by

$$\hat{\theta}_{k+1} = \hat{\theta}_k + \alpha\varphi(x_k)\tilde{x}_{k+1}^T - \Gamma\left\|I - \alpha\varphi(x_k)\varphi^T(x_k)\right\|\hat{\theta}_k. \tag{14}$$

Then the estimation error of the buffer length, $\tilde{x}_k$, and the modeling parameter error, $\tilde{\theta}_k$, are UUB, provided the design parameters are selected as follows

$$\begin{array}{c} \alpha\left\|\varphi(x_k)\right\|^2 < 1 \\ 0 < \Gamma < 1 \\ L_M < 1/\sqrt{\bar{\sigma}} \end{array}, \tag{15}$$

where L_M is the maximum singular value of the gain matrix L and $\bar{\sigma}$ is given by (11).

Proof: The proof is similar to that of Theorem 1 and is briefly presented below. Select the Lyapunov function as

$$V_k = V_1 + V_2, \text{ where } V_1 = \tilde{x}_k^T\tilde{x}_k \text{ and } V_2 = \alpha^{-1}tr\left\{\tilde{\theta}_k^T\tilde{\theta}_k\right\}. \tag{16}$$

Then substituting the tracking error dynamics (7) into V_1 yields the difference

$$\begin{aligned}\Delta V_1 &= \tilde{x}_{k+1}^T\tilde{x}_{k+1} - \tilde{x}_k^T\tilde{x}_k \\ &= \tilde{x}_k^T\left(L^TL - I\right)\tilde{x}_k + \varphi^T(x_k)\tilde{\theta}_k\tilde{\theta}_k^T\varphi(x_k) + \beta_{1,k}^T\beta_{1,k}\,, \\ &\quad +2\tilde{x}_k^TL^T\tilde{\theta}_k^T\varphi(x_k) + 2\tilde{x}_k^TL^T\beta_{1,k} + 2\varphi(x_k)\tilde{\theta}_k\beta_{1,k}\end{aligned} \tag{17}$$

where $\beta_{1,k} = \varepsilon_k + d_k + w_k$. Substituting the modeling parameter error update law (9) into V_2 yields the first difference

$$\begin{aligned}\Delta V_2 &= \alpha^{-1}tr\left\{\tilde{\theta}_{k+1}^T\tilde{\theta}_{k+1} - \tilde{\theta}_k^T\tilde{\theta}_k\right\} \\ &= \alpha^{-1}tr\left\{\begin{array}{l}\tilde{\theta}_k^T\beta_{2,k}^T\beta_{2,k}\tilde{\theta}_k - \tilde{\theta}_k^T\tilde{\theta}_k + \alpha^2\varphi(x_k)\varphi^T(x_k)\beta_{1,k}\beta_{1,k}^T \\ +\Gamma^2\left\|\beta_{2,k}\right\|^2\hat{\theta}_k^T\hat{\theta}_k - 2\alpha\Gamma\beta_{1,k}\varphi^2(x_k)\left\|\beta_{2,k}\right\|\hat{\theta}_k^T + 2\Gamma\tilde{\theta}_k^T\beta_{2,k}^T\left\|\beta_{2,k}\right\|\hat{\theta}_k\end{array}\right\}\end{aligned} \tag{18}$$

where $\beta_{2,k} = I - \alpha\varphi(x_k)\varphi^T(x_k)$.

Combining (17) and (18) and completing the squares for $\left\|\tilde{\theta}_k\right\|$, one obtains

$$\begin{aligned}\Delta V \le &-\left(\left(1-\bar{\sigma}L_M^2\right)\left\|\tilde{x}_k\right\|^2 - 2\gamma_1L_M\beta_M\left\|\tilde{x}_k\right\| - \gamma_2\right) \\ &-\beta_{3,k}\left\|\tilde{\theta}_k^T\varphi(x_k) - \beta_{3,k}^{-1}K\tilde{x}_k + \left(1-\beta_{3,k}+\Gamma\left\|\beta_{2,k}\right\|\right)\beta_M\right\|^2, \\ &-\alpha^{-1}\left\|\beta_{2,k}\right\|^2\Gamma(2-\Gamma)\left(\left\|\tilde{\theta}_k\right\| - \frac{1-\Gamma}{2-\Gamma}\theta_M^2\right)^2\end{aligned} \tag{19}$$

where

$$\gamma_1 = 1 + \left(1-\alpha\varphi_M^2\right)^{-1}\left(\Gamma\left(1-\alpha\varphi_M^2\right) + \alpha\varphi_M^2\right),$$

$$\begin{aligned}\gamma_2 = &\left(1 + \alpha\varphi_M^2 + \left(1-\alpha\varphi_M^2\right)^{-1}\left(\Gamma\left(1-\alpha\varphi_M^2\right) + \alpha\varphi_M^2\right)\right)^2\beta_M^2 \\ &+2\Gamma\left(1-\alpha\varphi_M^2\right)\varphi_M\theta_M\beta_M + \Gamma\left(\alpha(2-\Gamma)\right)^{-1}\left(1-\alpha\varphi_M^2\right)\theta_M^2\end{aligned},$$

$$\beta_{3,k} = 1 - \alpha\varphi^T(x_k)\varphi(x_k)\text{, and } \beta_M = \varepsilon_M + d_M + w_M\,.$$

Therefore we have $\Delta V \le 0$ as long as (10) and

$$\left\|\tilde{x}_k\right\| > \Upsilon_1, \tag{20}$$

where $\Upsilon_1 = \dfrac{\gamma_1 L_M \beta_M + \sqrt{\gamma_1^2 L_M^2 \beta_M^2 + \gamma_2 \left(1-\bar{\sigma} L_M^2\right)}}{1-\bar{\sigma} L_M^2}$. Similarly, combining (17) and (18) and completing the squares for $\|\tilde{x}_k\|$, one obtains

$$\begin{aligned}\Delta V \le & -\left(1-\bar{\sigma} L_M^2\right)\left(\|\tilde{x}_k\|^2 - \frac{\gamma_1 L_M \beta_M}{1-\bar{\sigma} L_M^2}\right)^2 - \beta_{3,k}\left\|\tilde{\theta}_k^T \varphi(x_k) - \beta_{3,k}^{-1} L \tilde{x}_k + \left(1-\beta_{3,k}+\Gamma\left\|\beta_{2,k}\right\|\right)\beta_M\right\|^2 \\ & -\alpha^{-1}\left\|\beta_{2,k}\right\|^2\left(\Gamma(2-\Gamma)\left\|\tilde{\theta}_k\right\|^2 - 2\Gamma(1-\Gamma)\theta_M\left\|\tilde{\theta}_k\right\| - \gamma_3\right)\end{aligned}, \quad (21)$$

where $\gamma_3 = \Gamma^2 \theta_M^2 + \dfrac{\alpha}{\left(1-\alpha\varphi_M^2\right)^2}\left(\begin{array}{l}\dfrac{L_M^2 \gamma_1^2 \beta_M^2}{1-\bar{\sigma} L_M^2} + 2\Gamma\left(1-\alpha\varphi_M^2\right)\varphi_M \theta_M \beta_M \\ +\beta_M^2\left(1+\alpha\varphi_M^2 + \left(1-\alpha\varphi_M^2\right)^{-1}\left(\Gamma\left(1-\alpha\varphi_M^2\right)+\alpha\varphi_M^2\right)\right)^2\end{array}\right)$.

Then we have $\Delta V \le 0$ as long as (10) and the following condition for $\tilde{\theta}_k$ hold

$$\left\|\tilde{\theta}_k\right\| > \frac{\Gamma(1-\Gamma)\theta_M + \sqrt{\Gamma^2(1-\Gamma)^2\theta_M^2 + \Gamma(2-\Gamma)\gamma_3}}{\Gamma(2-\Gamma)} . \quad (22)$$

Therefore, ΔV becomes less than zero once the estimation error exceeds the threshold in (20) or the parameter error exceeds the threshold in (22). That means that the estimation error of the buffer length and the modeling parameter error converge to a small subset with the proposed update law (14).

2.4. ATTACK DETECTION AND ESTIMATION

In the previous section, we have shown that the estimation error of the buffer length and the modeling parameter error converge to a small compact subset. Based on the results, the attack detectability condition is derived. Upon the detection of the attacks, another NN is deployed in order to estimate the flow injected by the attacker. It is shown that the modeling parameter error of the attack flow also converges to a small compact subset.

Theorem 3 (Attack Detectability Condition): Consider the flow model at the bottleneck node described by (1) and the observer described by (12). Attacks can be detected if the injected (dropped) flow w_k satisfies

$$\left\|\sum_{i=0}^{k-1}K^{k-i-1}w_k\right\| > \Upsilon_1 + \left\|\sum_{i=0}^{k-1}K^{k-i-1}\left(\tilde{\theta}_k^T\varphi(x_k)+\varepsilon_k+d_k\right)\right\| . \tag{23}$$

Proof: The solution of the error dynamics (13) is given by

$$\tilde{x}_k = \sum_{i=0}^{k-1}K^{k-i-1}\left(\tilde{\theta}_k^T\varphi(x_k)+\varepsilon_k+d_k+w_k\right). \tag{24}$$

If (23) is satisfied, by triangle inequality we have

$$\begin{aligned}\|\tilde{x}_k\| &\geq \left\|\sum_{i=0}^{k-1}K^{k-i-1}w_k\right\| - \left\|\sum_{i=0}^{k-1}K^{k-i-1}\left(\tilde{\theta}_k^T\varphi(x_k)+\varepsilon_k+d_k\right)\right\| \\ &> \Upsilon_1 + \left\|\sum_{i=0}^{k-1}K^{k-i-1}\left(\tilde{\theta}_k^T\varphi(x_k)+\varepsilon_k+d_k\right)\right\| - \left\|\sum_{i=0}^{k-1}K^{k-i-1}\left(\tilde{\theta}_k^T\varphi(x_k)+\varepsilon_k+d_k\right)\right\| \\ &= \Upsilon_1\end{aligned} . \tag{25}$$

Remark 1: The detectability condition proposed in Theorem 3 is a theoretical condition under which class of attack flows can be detected. However, this is not the way how the attack is detected in practice. Instead, the network detection residual is constantly monitored and the attack is detected once the residual exceeds the bound given by (20) due to attack input and as shown in the first part of Theorem 4.

Upon detecting the attack given in terms of bounded traffic flow input, this theorem also shows that the buffer flow estimation error and parameter estimation error are bounded.

Theorem 4 (Attack Estimation): Consider the flow model at the bottleneck node described by (1) and the observer described by (12). Assume that the attack flow can be modeled as $w_k = \theta_{w,k}^T\varphi_w(x_k)+\varepsilon_{w,k}$ where $\theta_{w,k}$, $\varphi_w(\cdot)$ and $\varepsilon_{w,k}$ is the weight vector, activation function and the modeling error of the attack flow respectively. Then attacks can be

detected when the network detection residual exceeds a predefined threshold given by (20). Upon detecting the attack, apply the following observer given by

$$\hat{x}_{k+1} = \hat{\theta}_k^T \varphi(x_k) + Tu_k - L_w(x_k - \hat{x}_k) + \hat{\theta}_{w,k}^T \varphi_w(x_k), \tag{26}$$

where L_w is the feedback gain matrix. $\hat{\theta}_k$ is the estimation of the weights vector for the unknown nonlinear function f which is updated by

$$\hat{\theta}_{k+1} = \hat{\theta}_k + \alpha_1 \varphi(x_k) \tilde{x}_{k+1}^T - \Gamma_1 \left\| I - \alpha_1 \varphi(x_k) \varphi^T(x_k) \right\| \hat{\theta}_k \ . \tag{27}$$

Similarly, $\hat{\theta}_{w,k}$ is the estimation of the weights vector for the attack flow and it is tuned using

$$\hat{\theta}_{w,k+1} = \hat{\theta}_{w,k} + \alpha_2 \varphi_w(x_k) \tilde{x}_{k+1}^T - \Gamma_2 \left\| I - \alpha_2 \varphi_w(x_k) \varphi_w^T(x_k) \right\| \hat{\theta}_{w,k} \tag{28}$$

Then the estimation error of the buffer length $\tilde{x}_k$, the modeling parameter error $\tilde{\theta}_k$, and the modeling parameter error of the attack flow $\tilde{\theta}_{w,k}$ are UUB, if the following conditions are satisfied:

$$0 < \alpha < \frac{1}{12} \min\left\{ \left\| \varphi(x_k) \right\|^2, \left\| \varphi_w(x_k) \right\|^2 \right\} \ , \tag{29}$$

$$\begin{aligned} 0 < \alpha_1 < \frac{1}{\sqrt{15}} \left\| \varphi(x_k) \right\| \left\| \varphi_w(x_k) \right\| \\ 0 < \alpha_2 < \frac{1}{\sqrt{15}} \left\| \varphi(x_k) \right\| \left\| \varphi_w(x_k) \right\| \end{aligned}, \tag{30}$$

$$\begin{aligned} \frac{1 - 1/\sqrt{15}}{\left\| I - \alpha_1 \varphi(x_k) \varphi^T(x_k) \right\|} < \Gamma_1 < \frac{1}{\left\| I - \alpha_1 \varphi(x_k) \varphi^T(x_k) \right\|} \\ \frac{1 - 1/\sqrt{15}}{\left\| I - \alpha_2 \varphi_w(x_k) \varphi_w^T(x_k) \right\|} < \Gamma_2 < \frac{1}{\left\| I - \alpha_2 \varphi_w(x_k) \varphi_w^T(x_k) \right\|} \end{aligned}, \tag{31}$$

$$L_{w,M} < \sqrt{\frac{\alpha}{4\alpha + 5\alpha_1 \left\| \varphi(x_k) \right\|^2 + 5\alpha_2 \left\| \varphi_w(x_k) \right\|^2}} \ , \tag{32}$$

where α, α_1, α_2, Γ_1, and Γ_2 are design parameters.

Proof: Select the Lyapunov function as

$$V_k = V_1 + V_2 + V_3, \tag{33}$$

where $V_1 = \alpha tr\left\{\tilde{x}_k^T \tilde{x}_k\right\}$, $V_2 = tr\left\{\tilde{\theta}_k^T \tilde{\theta}_k\right\}$, and $V_3 = tr\left\{\tilde{\theta}_{w,k}^T \tilde{\theta}_{w,k}\right\}$. Substituting (26) into (1) yields the state estimation error dynamics

$$\tilde{x}_{k+1} = L_w \tilde{x}_k + \tilde{\theta}_k^T \varphi(x_k) + \tilde{\theta}_{w,k}^T \varphi_w(x_k) + \beta_{4,k}, \tag{34}$$

where $\beta_{4,k} \triangleq d_k + \varepsilon_k + \varepsilon_{w,k}$

Applying the Cauchy-Schwarz inequality, we have

$$\begin{aligned} \Delta V_1 &\le -\alpha \left\|\tilde{x}_k\right\|^2 + \alpha tr\begin{Bmatrix} 4\tilde{x}_k^T L_w^T L_w \tilde{x}_k + 4\varphi^T(x_k)\tilde{\theta}_k^T \varphi(x_k) \\ +4{\varphi_w}^T(x_k)\tilde{\theta}_{w,k}\tilde{\theta}_{w,k}^T \varphi_w(x_k) + 4\beta_{4,k}^T \beta_{4,k} \end{Bmatrix} \\ &\le -\left(\alpha - 4\alpha L_{w,M}^2\right)\left\|\tilde{x}_k\right\|^2 + 4\alpha\left\|\varphi(x_k)\right\|^2\left\|\tilde{\theta}_k\right\|^2 + 4\alpha\left\|\varphi_w(x_k)\right\|^2\left\|\tilde{\theta}_{w,k}\right\|^2 + 4\alpha\left\|\beta_{4,k}\right\|^2 \end{aligned} \tag{35}$$

where $L_{w,M}$ is the maximum eigenvalue of the gain matrix L_w.

Combining the update law (27) and the state estimation error dynamics (26) yields

$$\begin{aligned} \tilde{\theta}_{k+1} &= \tilde{\theta}_k - \alpha_1 \varphi(x_k)\left(L_w \tilde{x}_k + \tilde{\theta}_k^T \varphi(x_k) + \tilde{\theta}_{w,k}^T \varphi_w(x_k) + \beta_{4,k}\right)^T - \Gamma_1\left\|I - \alpha_1 \varphi(x_k)\varphi^T(x_k)\right\|\hat{\theta}_k \\ &= \left(1 - \left\|I - \alpha_1 \varphi(x_k)\varphi^T(x_k)\right\|\right)\tilde{\theta}_k - \alpha_1 \varphi(x_k)\tilde{x}_k^T L_w^T - \alpha_1 \varphi(x_k)\varphi_w^T(x_k)\tilde{\theta}_{w,k} - \alpha_1 \varphi(x_k)\beta_{4,k}^T \\ &\quad + \Gamma_1\left\|I - \alpha_1 \varphi(x_k)\varphi^T(x_k)\right\|\theta_k \end{aligned} \tag{36}$$

Applying the Cauchy-Schwarz inequality yields

$$\begin{aligned} \Delta V_2 \le &-\left\|\tilde{\theta}_k\right\|^2 + 5\Psi_1^2\left\|\tilde{\theta}_k\right\|^2 + 5L_{w,M}^2\alpha_1^2\left\|\varphi(x_k)\right\|^2\left\|\tilde{x}_k\right\|^2 + 5\alpha_1^2\left\|\varphi(x_k)\right\|^2\left\|\varphi_w(x_k)\right\|^2\left\|\tilde{\theta}_{w,k}\right\|^2 \\ &+5\alpha_1^2\left\|\varphi(x_k)\right\|^2\left\|\beta_{4,k}^T\right\|^2 + 5\Gamma_1^2\left\|I - \alpha_1 \varphi(x_k)\varphi^T(x_k)\right\|^2\theta_M^2 \end{aligned}, \tag{37}$$

where $\Psi_1 \triangleq 1 - \Gamma_1\left\|I - \alpha_1 \varphi(x_k)\varphi^T(x_k)\right\|$.

Similarly, we have

$$\begin{aligned} \Delta V_3 \le &-\left\|\tilde{\theta}_{w,k}\right\|^2 + 5\Psi_2^2\left\|\tilde{\theta}_{w,k}\right\|^2 + 5L_{w,M}^2\alpha_2^2\left\|\varphi_w(x_k)\right\|^2\left\|\tilde{x}_k\right\|^2 + 5\alpha_2^2\left\|\varphi_w(x_k)\right\|^2\left\|\varphi(x_k)\right\|^2\left\|\tilde{\theta}_k\right\|^2 \\ &+5\alpha_2^2\left\|\varphi_w(x_k)\right\|^2\left\|\beta_{4,k}^T\right\|^2 + 5\Gamma_2^2\left\|I - \alpha_2 \varphi_w(x_k)\varphi_w^T(x_k)\right\|^2\theta_{w,M}^2 \end{aligned} \tag{38}$$

where $\Psi_2 \triangleq 1-\Gamma_2\left\|I-\alpha_2\varphi_w(x_k)\varphi_w^T(x_k)\right\|$.Combining (35), (37) and (38), one obtains

$$\begin{aligned}\Delta V &= \Delta V_1+\Delta V_2+\Delta V_3\\ &\le -\left(\alpha-4\alpha L_{w,M}^2-5L_{w,M}^2\alpha_1^2\left\|\varphi(x_k)\right\|^2-5L_{w,M}^2\alpha_2^2\left\|\varphi_w(x_k)\right\|^2\right)\left\|\tilde{x}_k\right\|^2\\ &\quad -\left(1-4\alpha\left\|\varphi(x_k)\right\|^2-5\Psi_1^2-5\alpha_2^2\left\|\varphi_w(x_k)\right\|^2\left\|\varphi(x_k)\right\|^2\right)\left\|\tilde{\theta}_k\right\|^2\\ &\quad -\left(1-4\alpha\left\|\varphi_w(x_k)\right\|^2-5\Psi_2^2-5\alpha_1^2\left\|\varphi(x_k)\right\|^2\left\|\varphi_w(x_k)\right\|^2\right)\left\|\tilde{\theta}_{w,k}\right\|^2+\Lambda\end{aligned}, \tag{39}$$

where $\Lambda \triangleq \left(4\alpha+4\alpha_1^2\left\|\varphi(x_k)\right\|^2+4\alpha_2^2\left\|\varphi_w(x_k)\right\|^2\right)\left\|\beta_{4,k}\right\|^2 +5\Gamma_1^2\left\|I-\alpha_1\varphi(x_k)\varphi^T(x_k)\right\|^2\theta_M^2+5\Gamma_2^2\left\|I-\alpha_2\varphi_w(x_k)\varphi_w^T(x_k)\right\|^2\theta_{w,M}^2$.

If inequality (32) is satisfied, then the first term in (39) is negative. If inequalities (29) through (31) are satisfied, we have

$$\begin{aligned}&4\alpha\left\|\varphi(x_k)\right\|^2<\frac{1}{3},\quad 5\Psi_1^2<\frac{1}{3},\quad 5\alpha_2^2\left\|\varphi_w(x_k)\right\|^2\left\|\varphi(x_k)\right\|^2<\frac{1}{3}\\ &4\alpha\left\|\varphi_w(x_k)\right\|^2<\frac{1}{3},\quad 5\Psi_2^2<\frac{1}{3},\quad 5\alpha_1^2\left\|\varphi(x_k)\right\|^2\left\|\varphi_w(x_k)\right\|^2<\frac{1}{3}\end{aligned} \tag{40}$$

Then the second and the third terms in (39) are also negative. Furthermore, since $\varphi(x_k)$, $\varphi_w(x_k)$, $\beta_{4,k}$, Ψ_1 and Ψ_2 are all bounded, the last term in (39), Λ, is also bounded, i.e., $\|\Lambda\|\le\Lambda_M$. Thus, we have $\Delta V<0$ in a compact set as long as inequalities (29) though (32) hold, and the following conditions are satisfied:

$$\begin{aligned}&\left\|\tilde{x}_k\right\|^2>\Lambda\Big/\begin{pmatrix}\alpha-4\alpha L_{w,M}^2-5L_{w,M}^2\alpha_1^2\left\|\varphi(x_k)\right\|^2\\ -5L_{w,M}^2\alpha_2^2\left\|\varphi_w(x_k)\right\|^2\end{pmatrix}\ \text{or}\ \left\|\tilde{\theta}_k\right\|^2>\Lambda\Big/\begin{pmatrix}1-4\alpha\left\|\varphi(x_k)\right\|^2-5\Psi_1^2\\ -5\alpha_2^2\left\|\varphi_w(x_k)\right\|^2\left\|\varphi(x_k)\right\|^2\end{pmatrix}\\ &\text{or}\ \left\|\tilde{\theta}_{w,k}\right\|^2>\Lambda\Big/\begin{pmatrix}1-4\alpha\left\|\varphi_w(x_k)\right\|^2-5\Psi_2^2\\ -5\alpha_1^2\left\|\varphi(x_k)\right\|^2\left\|\varphi_w(x_k)\right\|^2\end{pmatrix}.\end{aligned} \tag{41}$$

Therefore, the modeling parameter error $\tilde{\theta}_k$, and the modeling parameter error of the attack flow $\tilde{\theta}_{w,k}$ are UUB.

3. ATTACK DETECTION FOR PHYSICAL SYSTEMS

In this section, we first revisit a stochastic event-triggered optimal control scheme [29] for a class of nonlinear systems in the presence network-induced delays and packet losses. An event triggered control scheme is proven to reduce network traffic which might help to mitigate congestion in the presence of attacks in the event that attacks increase traffic flow. Next, since a large delay could lead to the instability of the system, the maximum overall delay that the physical system can tolerate is derived. At last, we present the proposed a detection scheme for attacks on the physical system.

3.1. PHYSICAL SYSTEM DYNAMICS

Consider the stochastic nonlinear continuous-time system described by

$$\dot{x}_p(t) = f_p(x_p(t)) + \gamma(t) g(x_p(t)) u_p(t - \tau(t)) + w_p(x_p(t)), \tag{42}$$

where $x_p(t) \in \Re^n$, $u_p(t) \in \Re^m$, and $w_p(x_p(t)) \in \Re^n$ is the system state, controller input, and attack input vector, respectively. The subscript "p" standing for "physical system" is utilized to differentiate the variable used to denote the network. The nonlinear functions $f_p(x(t)) \in \Re^n$ and $g_p(x(t)) \in \Re^{n \times m}$ are considered as unknown with $f_p(0) = 0$ and $x = 0$ being the unique equilibrium point. In particular, the notation $\tau(t)$ stands for the network-induced sensor-to-controller delay and $\gamma(t) \in \Re^{n \times n}$ is the packet loss indicator which equals to the identity matrix when the packet is received and the null matrix when the packet is lost.

Remark 2: The term $w_p(x_p(t))$ is used to characterize the change in system states caused by attacks on the sensors or actuators. Attacks on the physical systems can be

detected if $w_p(x_p(t))$ satisfies certain condition. This will be discussed later in Section 3.3 after the healthy case, i.e., $w_p(x_p(t))=0$.

Assumption 2: Let assumptions (1-7) presented in [29] hold.

Let the augmented state be defined as $z_k=[x_{p,k}^T \quad u_{p,k-1}^T \quad \cdots \quad u_{p,k-\bar{d}}^T]^T \in \Re^{n+\bar{d}m}$ and discretizing system (42) within the sampling period $\left[kT_s,(k+1)T_s\right]$ yields the simplified system dynamics

$$z_{k+1}=F(z_k)+G(z_k)u_{p,k}+W_p(z_k), \tag{43}$$

where $F(z_k)\in\Re^{\bar{d}m+n}$ and $G(z_k)\in\Re^{(\bar{d}m+n)\times m}$ are the discretized system dynamics defined in [16] and $W_p(z_k)\in\Re^{\bar{d}m+n}$ is the discretized attack input function matrix.

The event-triggered control (ETC) from [29] is adopted in this paper due to benefits mentioned before. As illustrated in Figure 3.1, an NN-based adaptive model is utilized to estimate the state vector and to approximate the unknown system dynamics.

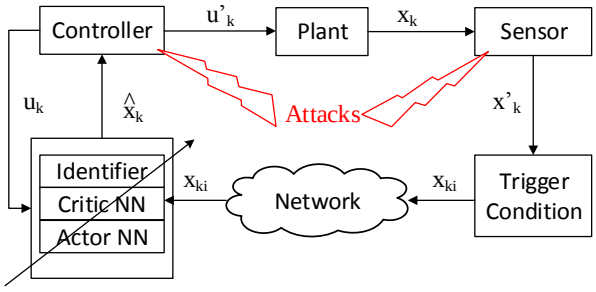


Figure 3.1. Structure of MBETC with attacks on the controller and sensor.

The sensor data will be sent to the controller only when the trigger condition is violated. Let $\breve{x}_k$ be the state vector held at the controller, which is given by

$$\breve{x}_k = x_{p,k_i}, \text{ for } k_i \le k < k_{i+1}, \tag{44}$$

with the event-triggered instant $\{k_i\}_{i=1}^{\infty}$ being the subsequence of sampling instants $k \in \mathbb{N}$. Then the augmented event sampled state vector becomes $\breve{z}_k = z_{k_i}$ with $\breve{z}_k = [\breve{x}_k^T \; u_{p,k-1}^T \cdots u_{p,k-\bar{d}}^T]^T$ and $z_{k_i} = [x_{p,k_i}^T \; u_{p,k_i-1}^T \; u_{p,k_i-\bar{d}}^T]^T$. The error between z_k and $\breve{z}_k$ can be expressed as

$$e_{ET,k} = z_k - \breve{z}_k, \tag{45}$$

where $e_{ET,k}$ is referred to as event sampling error. Let the infinite horizon stochastic value function in terms of the augmented state vector be given by

$$V_k = \underset{\tau,\gamma}{E}\left\{\sum_{j=k}^{\infty} z_j^T Q_z z_j + u_{p,j}^T R_z u_{p,j}\right\}, \; k = 0,1,2,\ldots, \tag{46}$$

where Q_z and R_z are positive definite (PD) penalty matrices. However, the optimal control input is usually difficult to obtain because: 1) it is very challenging to solve discrete time Hamilton-Jacobi-Bellman (HJB) equation; 2) the nonlinear matrix function $G(z_k)$ is unknown. Therefore, an NN-based solution [29] is adopted.

3.2. STOCHASTIC ETC DESIGN

The dynamics of system (43) can be written as

$$z_{k+1} = [F(z_k) \quad G(z_k)][1 \quad u_k^T]^T + W_p(z_k) = \underset{\tau,\gamma}{E}\{\theta_I^T \varphi_I(\breve{z}_k)\bar{u}_k + \bar{\varepsilon}_{e,I}(\breve{z}_k, e_{ET,k})\}, \tag{47}$$

where $\theta_I = [\theta_F^T \quad \theta_G^T]^T \in \Re^{(m+1)l_I \times (\bar{d}m+n)}$ is the constant target NN weights vector with θ_F and θ_G being the targets for the respective functions F and G. The activation function are selected as $\varphi_I(\breve{z}_k) = diag\{\varphi_F(\breve{z}_k) \; \varphi_G(\breve{z}_k)\}$ and $\varphi_F(\breve{z}_k) \in \Re^{l_I}$, $\varphi_G(\breve{z}_k) \in \Re^{ml_I \times m}$ with l_I being the number of

neurons. The vector $\bar{u}_k = [1 \;\; u_{p,k}^T]^T$ is the augmented control input and $\bar{\varepsilon}_{e,I}(\breve{z}_k, e_{ET,k}) = \theta_I^T[\varphi_I(\breve{z}_k + e_{ET,k}) - \varphi_I(\breve{z}_k)]\bar{u}_k + \bar{\varepsilon}_I(\breve{z}_k + e_{ET,k}) + W_p(z_k)$ is the event sampled reconstruction error where $\bar{\varepsilon}_I(\breve{z}_k + e_{ET,k}) = \varepsilon_I \bar{u}_k$ with $\varepsilon_I = [\varepsilon_F(z_k) \;\; \varepsilon_G(z_k)]$ being the NN reconstruction error.

Let the event-based identifier dynamics be defined as

$$\hat{z}_{k+1} = \hat{F}(\breve{z}_k) + \hat{G}(\breve{z}_k)u_{p,k} = \underset{\tau,\gamma}{E}\{\hat{\theta}_I^T \varphi_I(\breve{z}_k)\bar{u}_k\}, \tag{48}$$

with $\hat{\theta}_I$ being the NN weights of the identifier. Let the estimation error of the identifier be $\underset{\tau,\gamma}{E}\{\tilde{z}_k\} = \underset{\tau,\gamma}{E}\{z_k - \hat{z}_k\}$ and then one can get the error dynamics as

$$\underset{\tau,\gamma}{E}\{\tilde{z}_{k+1}\} = \underset{\tau,\gamma}{E}\left\{\begin{matrix}\tilde{\theta}_{I,k}^T \varphi_I(z_k)\bar{u}_k + \hat{\theta}_I^T[\varphi_I(z_k) - \varphi_I(\breve{z}_k)]\bar{u}_k \\ +\bar{\varepsilon}_I(z_k) + W_{p,k}(z_k)\end{matrix}\right\}. \tag{49}$$

The NN weights update law for the identifier is given by

$$\underset{\tau,\gamma}{E}\{\hat{\theta}_{I,k}\} = \underset{\tau,\gamma}{E}\left\{\hat{\theta}_{I,k-1} + \frac{\chi_k \alpha_I \varphi_I(\breve{z}_{k-1})\bar{u}_{k-1}\tilde{z}_{I,k}^T}{(\varphi_I(\breve{z}_{k-1})\bar{u}_{k-1})^T(\varphi_I(\breve{z}_{k-1})\bar{u}_{k-1}) + 1}\right\}, \tag{50}$$

with $\alpha_I > 0$ being the learning rate and χ_k being the event-trigger indicator which equals to one if the event is triggered and zero otherwise.

Similar to the previous subsection, define the critic NN estimation of the value function and the weights update law as

$$\hat{V}_k = \underset{\tau,\gamma}{E}\{\hat{\theta}_{V,k}^T \varphi_V(\breve{z}_k)\}, \tag{51}$$

$$\underset{\tau,\gamma}{E}\{\hat{\theta}_{V,k}\} = \underset{\tau,\gamma}{E}\left\{\hat{\theta}_{V,k-1} - \frac{\chi_k \alpha_V \Delta\varphi_V(\breve{z}_k)e_{V,k}}{\Delta\varphi_V^T(\breve{z}_k)\Delta\varphi_V(\breve{z}_k) + 1}\right\}, \tag{52}$$

where $\alpha_V > 0$ is the learning rate and $\Delta\varphi_V(\breve{z}_k) \triangleq \varphi_V(\breve{z}_{k+1}) - \varphi_V(\breve{z}_k)$. The estimated optimal control input and the NN weight update law are defined as

$$u_k = \underset{\tau,\gamma}{E}\{\hat{\theta}_{u,k}^T \varphi_u(\breve{z}_k)\}, \tag{53}$$

$$\underset{\tau,\gamma}{E}\{\hat{\theta}_{u,k}\} = \underset{\tau,\gamma}{E}\left\{\hat{\theta}_{u,k-1} - \frac{\chi_k \alpha_u \varphi_u(\breve{z}_{k-1}) e_{u,k-1}^T}{\varphi_u^T(\breve{z}_{k-1})\varphi_u(\breve{z}_{k-1})+1}\right\}. \tag{54}$$

where $\alpha_u > 0$ is the learning rate. The event-trigger condition design is critical because on one hand, excessive triggering clearly deviates from the original intention of reducing the data transmission. On the other hand, insufficient triggering will result in a regulation error, thus degrading the performance and even leading to the instability of the system. Here, the adaptive event-trigger condition is given by [29]

$$\sigma_{ET,k}\ D\left(\left\|\underset{\tau,\gamma}{E}\{e_{ET,k}\}\right\|^2\right) > \rho_p \left\|\underset{\tau,\gamma}{E}\{z_k\}\right\|^2, \tag{55}$$

where $\sigma_{ET,k} = 12G_M^2 C_{\varphi_u}^2 \left\|\underset{\tau,\gamma}{E}\{\hat{\theta}_{u,k}\}\right\|^2 + C_{\varphi_I} \left\|\underset{\tau,\gamma}{E}\{\hat{\theta}_{I,k}\}\right\|^2$ with, $0 < \Gamma < 1$, $\rho_p = 2\Gamma(1-2\mu_p)$, $0 < \mu_p < 1/2$ and G_M is the upper bound of the matrix function $G(z_k)$. The function $D(\cdot)$ is the dead zone operator defined as $D(x) = 0$ when $\left\|\underset{\tau,\gamma}{E}\{z_k\}\right\| > B_z$ and $D(x) = x$ otherwise with B_z being the UB of the system state. Now the boundedness of the system under healthy case when there are no attacks on the network and physical system are shown.

Theorem 5 [29]: Consider the system (43) with the event-trigger condition (45), NN identifier (48) with the weight update law (50), the critic NN (38) with the weights update law (52), and the actor NN (53) with the weights update law (54). Assume that there is no attack on the network and/or the physical system. Then there exist three constants $0 < \alpha_I < ½$, $0 < \alpha_V < ½$, $0 < \alpha_u < ¼$, and positive integer N such that $\underset{\tau,\gamma}{E}\{z_k\}$, $\underset{\tau,\gamma}{E}\{\tilde{\theta}_{I,k}\}$, $\underset{\tau,\gamma}{E}\{\tilde{\theta}_{V,k}\}$, and $\underset{\tau,\gamma}{E}\{\tilde{\theta}_{u,k}\}$ are ultimately bounded in the mean for all $k_i > k_0 + N$. Further, the estimated optimal value function and control input converge close to their respective optimal values.

In the above analysis, we consider the case where the communication network is in healthy condition, i.e., the delays and packet losses are bounded by a small value. However, the delays and packet losses increase in the presence of attacks on the network and lead to instability of the physical system. Therefore, it is of interest to determine the maximum delays and packet losses that the physical system can tolerate.

Let $\left[k,\quad k+\varepsilon_{p,k}\right]$ be the interval during which there is no sensor data received at the controller. Then the value of $\varepsilon_{p,k}$ depends on the following three factors: the event-trigger error, network-induced delays and packet losses. This can be explained with the following simplified example. Suppose the event is triggered at $k=0$ and the controller received the event with no delay. The next event is triggered at $k=3$ however the packet containing this event is lost. Then the event will be triggered again at $k=4$ since the control input has not been changed and the trigger error keeps increasing. Suppose that the network-induced delay is $\tau=2T_s$, then the time that the controller receives the event will be $k=6$. Therefore, in this case we have $\varepsilon_{p,k}=6T_s$. The following theorem gives the maximum timespan $\varepsilon_{p,k}$ that the physical system can tolerate.

Theorem 6: Consider the nonlinear discrete-time system (43) without physical attacks i.e. $W_p(z_k)=\mathbf{0}$. Assume the communication network is under attack such that the timespan $\varepsilon_{p,k}$ is always greater than ε_m. Then the physical system becomes unstable if ε_m satisfies

$$r\underset{\tau,\gamma}{E}\left\{\left\|z_{\varepsilon_m+k_i}-z_{k_i}\right\|^2\right\}>E\left\{HZ_k-B_{\tilde{\theta},k}^{c2}\right\}, \tag{56}$$

where $r=6G_M^2C_{\varphi_u}^2\left\|\underset{\tau,\gamma}{E}\{\hat{\theta}_{u,k}\}\right\|^2+C_{\varphi_I}\left\|\underset{\tau,\gamma}{E}\{\hat{\theta}_{I,k}^T\}\right\|^2/2$,

$$B_{\tilde{\theta},k}^{c2} = 6G_M^2\varphi_{u,M}^2\left\|E_{\tau,\gamma}\{\tilde{\theta}_{u,k}\}\right\|^2 + (1/2)\varphi_{I,M}\left\|E_{\tau,\gamma}\{\tilde{\theta}_{I,k}\}\right\|^2 + (\varphi_{I,M} + C_{\varphi_I})\varphi_{u,M}\left\|E_{\tau,\gamma}\{\tilde{\theta}_{u,k}\}\right\|^2 +$$

$(1/2)(\varphi_{I,M} + C_{\varphi_I}) + \varphi_{I,M}\varphi_{u,M}\theta_{u,M}^2$, $H = [(1-2\mu) \quad I]$, and $Z_k = \left[E\left\{\|z_k\|^2\right\} \quad E\left\{\|\tilde{z}_k\|^2\right\}\right]^T$.

Proof: Let the last event triggered time be k_i. Then if the timespan $\varepsilon_{p,k}$ is always greater than ε_m, there will be no NN weights updates nor control updates during the interval $(k_i, k_i + \varepsilon_m)$. Select the Lyapunov function as $V(z_k) = \underset{\tau,\gamma}{E}\{z_k^T z_k\} + \left\|E_{\tau,\gamma}\{\tilde{z}_k\}\right\|$. By substituting the system dynamics (47) and the estimation error dynamics (49) into the Lyapunov function and using the result from Theorem 5, one can get

$$\Delta V(z_k) \le r\left\|E_{\tau,\gamma}\{e_{ET,k}\}\right\|^2 - HZ_k + B_{\tilde{\theta},k}^{c2}, \tag{57}$$

Therefore if the event is not triggered for enough long time, the trigger error $e_{ET,k}$ will keep increasing and become the dominant one in (57) and thus $\Delta V(z_k)$. If (56) is satisfied, we have

$$r\left\|E_{\tau,\gamma}\{e_{ET,k}\}\right\|^2 - HZ_k + B_{\tilde{\theta},k}^{c2} = r\,\underset{\tau,\gamma}{E}\left\{\left\|z_{\varepsilon_m+k_i} - z_{k_i}\right\|^2\right\} - HZ_k + B_{\tilde{\theta},k}^{c2} > 0$$

Hence the stability of the physical system cannot be guaranteed if $\varepsilon_{p,k} \ge \varepsilon_m$ always holds.

3.3. PHYSICAL ATTACK DETECTION

In this section, we introduce the attack detection scheme on the physical system. The idea is to monitor the state estimation error of the physical system, which is the difference between the measured and the estimated physical system state generated by the identifier. Since it is shown in Theorem 5 that the expected estimation error is UB under healthy condition, it will exceed the bound in the presence of an attack and thus the attack

can be detected. Similar to Theorem 3, the following theorem gives the detectability condition for attacks on the physical system.

Theorem 7: Consider the nonlinear discrete-time system (43). Let the identifier be defined as (48) with the NN weights update law shown in (50). Then attacks on the physical system can be detected at if $W_{p,k}$ satisfies

$$\underset{\tau,\gamma}{E}\left\{\left\|\tilde{\theta}_{I,k}^{T}\varphi_I(z_k)\bar{u}_k+\hat{\theta}_I^{T}[\varphi_I(z_k)-\varphi_I(\breve{z}_k)]\bar{u}_k+\bar{\varepsilon}_I(z_k)+W_p(z_k)\right\|\right\}>B_{\tilde{z},k}^{c2}, \tag{58}$$

Proof: Let the Lyapunov function be defined as

$$V(z_k)=\underset{\tau,\gamma}{E}\{z_k^{T}z_k\}+\left\|\underset{\tau,\gamma}{E}\{\tilde{z}_k\}\right\|. \tag{59}$$

Substitute the system dynamics (47) and the estimation error dynamics (49) into (59) and after some manipulation, one can get

$$\Delta V(z_k)\le-(1-2\mu)(1-\Gamma)\left\|\underset{\tau,\gamma}{E}\{z_k\}\right\|^2-\left\|\underset{\tau,\gamma}{E}\{\tilde{z}_k\}\right\|+B_{\tilde{\theta},k}^{c2}+\bar{\varepsilon}_{I,M}+6G_M^2\varepsilon_{u,M}^2. \tag{60}$$

Thus we have $\Delta V(z_k)<0$, as long as

$$\left\|\underset{\tau,\gamma}{E}\{\tilde{z}_k\}\right\|>B_{\tilde{z},k}^{c2}. \tag{61}$$

As a result, the estimation error in the absence of attacks is bounded by $B_{\tilde{z},k}^{c2}$. If (58) is satisfied, we have

$$\underset{\tau,\gamma}{E}\left\{\left\|\tilde{\theta}_{I,k}^{T}\varphi_I(z_k)\bar{u}_k+\hat{\theta}_I^{T}[\varphi_I(z_k)-\varphi_I(\breve{z}_k)]\bar{u}_k+\bar{\varepsilon}_I(z_k)+W_p(z_k)\right\|\right\}=\left\|\underset{\tau,\gamma}{E}\{\tilde{z}_{k_a}\}\right\|>B_{\tilde{z},k}^{c2}.$$

Therefore the expected estimation error exceeds the bound and thus the attack can be detected.

Next, upon detecting the attack on the physical systems, it is of interest to estimate the attacker input $W_p(z_k)$. In order to do this, we rewrite the system dynamics (47) as

$$z_{k+1} = \begin{bmatrix} F(z_k) & W_p(z_k) & G(z_k) \end{bmatrix} \begin{bmatrix} 1 & 1 & u_k^T \end{bmatrix}^T = \underset{\tau,\gamma}{E}\{\theta_{Iw}^T \varphi_I(\breve{z}_k)\bar{u}_{w,k} + \bar{\varepsilon}_{e,Iw}(\breve{z}_k, e_{ET,k})\}, \tag{62}$$

where $\theta_{Iw} = \begin{bmatrix} \theta_F^T & \theta_W^T & \theta_G^T \end{bmatrix}^T$ is the constant target NN parameter vector and $\bar{u}_{w,k} = \begin{bmatrix} 1 & 1 & u_k^T \end{bmatrix}^T$ is the augmented control input vector. The event sampled reconstruction error $\bar{\varepsilon}_{e,Iw}(\breve{z}_k, e_{ET,k})$ is then given by

$$\bar{\varepsilon}_{e,Iw}(\breve{z}_k, e_{ET,k}) = \theta_{Iw}^T \left(\varphi_I(\breve{z}_k + e_{ET,k}) - \varphi_I(\breve{z}_k)\right)\bar{u}_{w,k} + \bar{\varepsilon}_{Iw}(\breve{z}_k + e_{ET,k}), \tag{63}$$

$\bar{\varepsilon}_{Iw}(\breve{z}_k + e_{ET,k}) = \varepsilon_{Iw}\bar{u}_{w,k}$ with $\varepsilon_{Iw} = \begin{bmatrix} \varepsilon_F(z_k) & \varepsilon_W(z_k) & \varepsilon_G(z_k) \end{bmatrix}$ being the NN reconstruction error vector.

Accordingly, an NN-based approximator is added to (48) such that the dynamics of the identifier becomes

$$\hat{z}_{k+1} = \hat{F}(\breve{z}_k) + \hat{W}(\breve{z}_k) + \hat{G}(\breve{z}_k)u_{p,k} = \underset{\tau,\gamma}{E}\{\hat{\theta}_{Iw}^T \varphi_I(\breve{z}_k)\bar{u}_{w,k}\}, \tag{64}$$

where $\hat{\theta}_{Iw}$ being the NN weights of the identifier. Then the error dynamics of the identifier can be computed as

$$\underset{\tau,\gamma}{E}\{\tilde{z}_{k+1}\} = \underset{\tau,\gamma}{E}\left\{\tilde{\theta}_{Iw,k}^T \varphi_I(z_k)\bar{u}_{w,k} + \hat{\theta}_{Iw}^T[\varphi_I(z_k) - \varphi_I(\breve{z}_k)]\bar{u}_{w,k} + \bar{\varepsilon}_{Iw}(z_k)\right\}. \tag{65}$$

The following theorem shows that the expected value of the estimation error of the bounded attacker input $W_p(z_k)$ is UB.

Theorem 8: Consider the nonlinear discrete-time system (43) in the presence of the attack. Assume the attack is launched after the convergence of identifier (48) and is bounded by $\|W_p(z_k)\| \le W_{p,M}$. Suppose the vector $\tilde{\theta}_{Iw,k}\bar{u}_{w,k}$ satisfies the PE condition [29]. Then an attack can be detected when (61) is satisfied. Upon detecting the attack, apply the identifier given in (64) with the following update law

$$\underset{\tau,\gamma}{E}\{\hat{\theta}_{Iw,k}\}=\underset{\tau,\gamma}{E}\left\{\hat{\theta}_{Iw,k-1}+\frac{\chi_k\alpha_{Iw}\varphi_I(\bar{z}_{k-1})\bar{u}_{w,k-1}\tilde{z}_{I,k}^T}{(\varphi_I(\bar{z}_{k-1})\bar{u}_{w,k-1})^T(\varphi_I(\bar{z}_{k-1})\bar{u}_{w,k-1})+1}\right\}, \tag{66}$$

where $0<\alpha_{Iw}<1/2$ is the learning rate. Then, for a positive integer N_w the identifier NN weights estimation error $\underset{\tau,\gamma}{E}\left(\tilde{\theta}_{Iw,k}\right)$ is UB in the mean for all $k_i>k_0+N_w$.

Proof: Select the Lyapunov function $L_{Iw,k}=tr\left\{\underset{\tau,\gamma}{E}\{\tilde{\theta}_{Iw,k}^T\tilde{\theta}_{Iw,k}\}\right\}$. For the case of event sampled instants, we have $\bar{z}_k=z_k$, $\chi_k=1$ and $k=k_i$. Then the identifier estimation error dynamics becomes

$$\underset{\tau,\gamma}{E}\{\tilde{\theta}_{Iw,k+1}\}=\underset{\tau,\gamma}{E}\left\{\tilde{\theta}_{Iw,k}-\frac{\alpha_{Iw}\varphi_I(z_k)\bar{u}_{w,k}\tilde{z}_{I,k+1}^T}{(\varphi_I(z_k)\bar{u}_{w,k})^T(\varphi_I(z_k)\bar{u}_{w,k})+1}\right\}. \tag{67}$$

with

$$\tilde{z}_{k+1}=\tilde{\theta}_{wI,k}^T\varphi_I(z_k)\bar{u}_{w,k}+\bar{\varepsilon}_{wI,k}. \tag{68}$$

Substituting (67) into the Lyapunov function and computing the first difference yields

$$\begin{aligned}\Delta L_{I,k}=&-tr\left(\underset{\tau,\gamma}{E}\left\{\frac{2\alpha_{wI}\tilde{\theta}_{wI,k}^T\varphi_I(z_k)\bar{u}_{w,k}\tilde{z}_{I,k+1}^T}{(\varphi_I(z_k)\bar{u}_{w,k})^T(\varphi_I(z_k)\bar{u}_{w,k})+1}\right\}\right)\\&+tr\left(\underset{\tau,\gamma}{E}\left\{\frac{\alpha_{wI}^2\tilde{z}_{I,k+1}(\varphi_I(z_k)\bar{u}_{w,k})^T(\varphi_I(z_k)\bar{u}_{w,k})\tilde{z}_{I,k+1}^T}{((\varphi_I(z_k)\bar{u}_{w,k})^T(\varphi_I(z_k)\bar{u}_{w,k})+1)^2}\right\}\right).\end{aligned} \tag{69}$$

Substituting (68) into (69) and applying Cauchy-Schwartz inequality yields

$$\Delta L_{I,k}\le-\bar{\varphi}_{I,m}^2\alpha_{wI}(1-2\alpha_{wI})\left\|\underset{\tau,\gamma}{E}\{\tilde{\theta}_{wI,k}\}\right\|^2+(1+2\alpha_{wI})\alpha_{wI}\bar{\varepsilon}_{wI,M}^2, \tag{70}$$

where $0<\bar{\varphi}_{I,m}^2\le\min_k\left\{\frac{\left\|(\varphi_I(z_k)\bar{u}_{w,k})(\varphi_I(z_k)\bar{u}_{w,k})^T\right\|}{(\varphi_I(z_k)\bar{u}_{w,k})^T(\varphi_I(z_k)\bar{u}_{w,k})+1}\right\}$ is satisfied due to the PE condition [29].

Therefore, we have $\Delta L_{I,k}<0$ as long as

$$\left\|\underset{\tau,\gamma}{E}\{\tilde{\theta}_{wI,k}\}\right\|>\sqrt{(1+2\alpha_{wI})\bar{\varepsilon}_{wI,M}^2/\bar{\varphi}_{I,m}^2(1-2\alpha_{wI})}\triangleq B_{ub}^{\tilde{\theta}_{wI}}. \tag{71}$$

Therefore, $\underset{\tau,\gamma}{E}\left(\tilde{\theta}_{Iw,k}\right)$ is bounded at the event sampled instants. Now consider the case of the intervals between the event instants. Since the weights are not updated during the event instants, we have

$$\Delta L_{I,k} = tr\left(\underset{\tau,\gamma}{E}\{\tilde{\theta}_{wI,k+1}^{T}\tilde{\theta}_{wI,k+1}\}\right) - tr\left(\underset{\tau,\gamma}{E}\{\tilde{\theta}_{wI,k}^{T}\tilde{\theta}_{wI,k}\}\right) = 0 . \tag{72}$$

Therefore, we have $\left\|\underset{\tau,\gamma}{E}\{\tilde{\theta}_{wI,k_i+1}\}\right\| \le \left\|\underset{\tau,\gamma}{E}\{\tilde{\theta}_{wI,k_i}\}\right\|$ held for both cases. As a result, there exists a positive integer N_w such that for all $k_i > k_0 + N_w$ we have $\left\|\underset{\tau,\gamma}{E}\{\tilde{\theta}_{wI,k}\}\right\| \to B_{ub}^{\tilde{\theta}_{wI}}$. Therefore, the identifier NN weights estimation error $\underset{\tau,\gamma}{E}\left(\tilde{\theta}_{Iw,k}\right)$ is UB in the mean.

4. SIMULATION RESULTS

In order to show the effectiveness of the proposed attack detection scheme, simulations are performed in MATLAB with the following parameters for the communication network: sampling period $T = 1\text{ms}$, total simulation time $T_s = 200T$. Without the loss of generosity, let the desired number of packets in the bottleneck node be $x_{d,k} = 200 + 100\sin(k/25)$, the unknown nonlinear function be $f(x_k) = \sqrt{x_k}$, and the maximum modeling error or disturbance be $d_M = 5$. Past three values are used as the input to the one-layer NN as a tradeoff between approximation and computation. The logsig activation function is selected and all NN weights are initialized to zero.

In order to make the inequalities in (10) and (15) hold, the feedback gain K is selected as 0.05 and the coefficient of the adaptive term Γ is selected as 0.5. The initial adaptation gain α is taken as 0.1 and is updated using the projection algorithm as $\alpha_k = 0.5/\left(0.1 + \varphi^T(x_k)\varphi(x_k)\right)$.

A jamming attack in introduced at $t = 100\text{ms}$ and it aims at creating traffic congestion by placing jammers that consistently inject data into the link. Assuming the attacking strength (number of jammers) increases linearly, then the number of packets injected by the attacker can be modeled by $\omega_k = \alpha_w(k - k_0)$ where α_w is the attacking strength and k_0 is the attack launch time. In the simulation, we choose $\alpha_w = 20$ and $k_0 = 100$.

4.1. NETWORK SIMULATION

Figure 4.1 shows the actual and desired number of packets in the bottleneck node. Before the attack is launched, the actual number of packets fluctuates around the desired

value. Moreover, as shown in Figure 4.2, the modeling parameter error becomes very close to zero, which verifies the result given in Theorem 1.

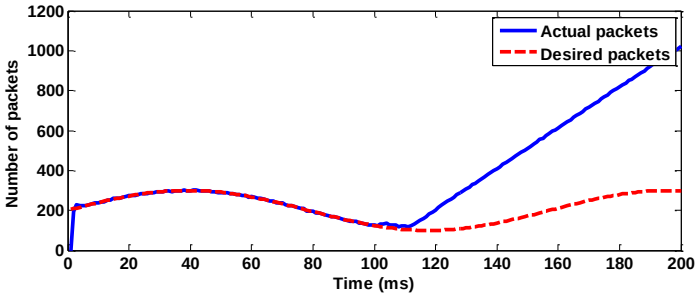


Figure 4.1. Actual and desired number of packets in the bottleneck node.

Figure 4.3 shows the estimation error and the attacker injected packets, when the observer given in Theorem 2 is applied.

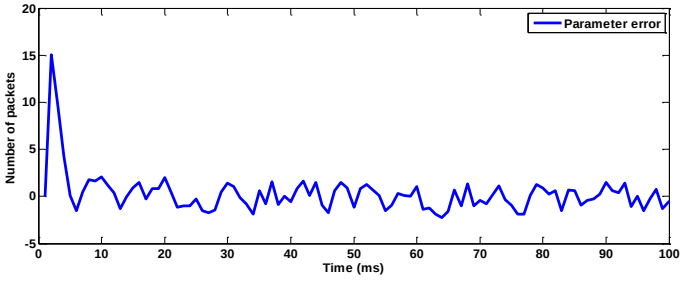


Figure 4.2. Parameter error for the number of packets before the attack is launched.

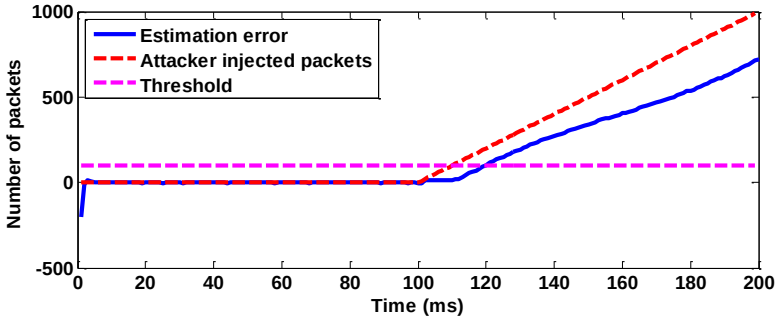


Figure 4.3. The estimation error and the attacker injected packets, when the observer given in Theorem 2 is applied.

Before the attack is launched, the estimation error is very close to zero, concluding that the estimated state given by the observer in Theorem 2 is fairly accurate. Once the attack is launched, the actual number of packets in the bottleneck node starts increasing and deviating from the desired value, as shown in Figure 4.1. As a result, the estimation error of the flow, plotted in Figure 4.3, exceeds the threshold shortly after the attack is launched and thus it can be detected, which proves the correctness of Theorem 3.

Next, we apply the new observer proposed in Theorem 4 in order to estimate the number of packets injected by the attacker. As plotted in Figure 4.4, the estimated number of packets injected by the attacker with the new observer converges to the actual value, which agrees with the conclusion of Theorem 4. With the estimated attack flow, one can estimate the delay and packet losses in the link, which can be further utilized to tune the controller parameters of the physical systems.

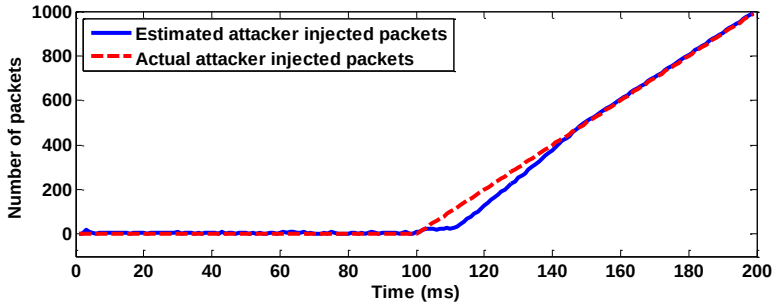


Figure 4.4. Estimated and actual number of packets injected by the attacker.

4.2. PHYSICAL SYSTEM

The following second-order nonlinear discrete system [29] is considered during the simulation

$$\begin{aligned} x_{1,k+1} &= x_{2,k}; \\ x_{2,k+1} &= \frac{x_{2,k}}{1+x_{1,k}^2} + \left(2+\sin\left(x_{1,k}\right)\right)u_k. \end{aligned} \tag{73}$$

The initial states are selected as $[-2,2]^T$ and the NN weights are initialized with random numbers in the interval $(0,1)$ with 15 neurons each in the hidden layer. The learning rate are selected as $\alpha = 0.24$ and $\kappa = 10^{-5}$. Based on the dynamics described in (73), we choose $g_{\min} = 1$ and $\Gamma = 0.99$. The sampling period T_s is 0.01 second and the total simulation time is 15 seconds. The time varying delay bound is $\bar{d} = 2$, the mean value of the delay is $\underset{\tau,\gamma}{E}(\tau) = 12ms$. The packet losses follow a Bernoulli distribution with the probability of dropping packets being $p = 0.1$.

First we consider the scenario where there are no attacks on either the physical system or the networks. As shown in Figure 4.5, the system states converge to close to zero after about seven seconds, although the initial states and the NN weights are fairly far from their target values.

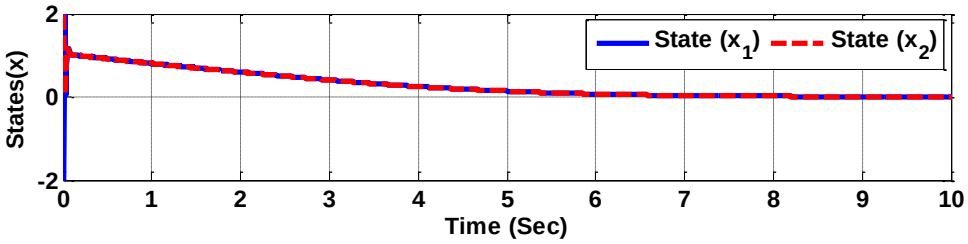


Figure 4.5. The convergence of the states when the network is healthy.

Figure 4.6 shows the evolution of the trigger condition threshold and the state estimation error. The state estimation error oscillates between zero and the trigger threshold due to the fact that in the event-trigger control scheme, the estimation error is set to zero once it becomes equal or greater than the trigger threshold. It can also be observed that state estimation error converges to close to zero after about 10 seconds and eventually stops satisfying the trigger condition due to the dead zone function. Therefore, Figure 4.5 and Figure 4.6 confirm Theorem 5.

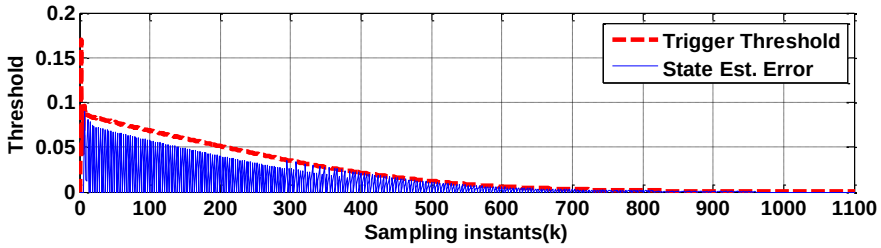


Figure 4.6. The evolution of trigger threshold and state estimation error.

Next, in order to verify that ETC scheme help reduce the network packet losses, black hole attack is introduced to the network. To be specific, we assume at each sampling instant, the attack drops the sensor-to-controller packet with the probability of 0.3. Figure 4.7 shows the comparison of the accumulated number of dropped packets between the event-triggered and time-driven control systems in the presence of black hole attack on the network. It can be observed that for the ETC, the number of dropped packets by the attack is much fewer than that of the time-driven system.

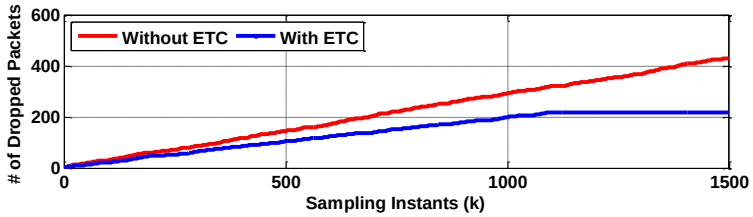


Figure 4.7. Number of dropped packets with and without ETC.

Especially when the event-trigger error is small enough (after 11s in this example) and the event is no longer triggered, there will be no data loss at all. Therefore, it is confirmed by Figure 4.7 that the ETC scheme reduces the packet losses in the presence of attacks.

At last, the jamming attack is introduced in the network and as a result, the overall delay exceeds the maximum value that the system can tolerate. In the simulation, we select $\varepsilon_m = 6T_s$ such the inequality (56) holds. Consequently, as shown in Figure 4.8, the system states do not converge to the origin, which is consistent with the analysis of Theorem 6.

Now, we introduce an attack on the physical system provided the network is in the normal condition. Assume the attack is launched at $t_{att} = 10s$ after the convergence of the system states. The attack targets by the modifying the sensor and the state x_2 such that

$$x_{2,k+1} = \frac{x_{2,k}}{1+x_{1,k}^2} + \left(2+\sin\left(x_{1,k}\right)\right)u_k + \beta_{att}\left(k - t_{att}\right)$$

where β_{att} is the attacking strength and is selected as 0.1 in the simulation.

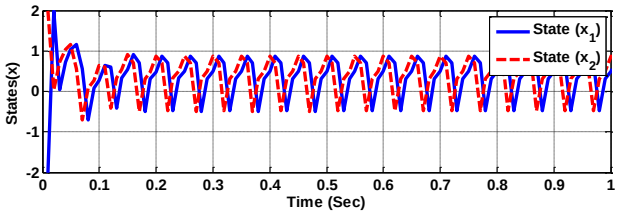


Figure 4.8. The system states when overall delay exceeds the threshold.

As shown in Figure 4.9, the estimation error increases after the launch of the attack and exceeds the detection threshold shortly. As a result, the attack can be detected, which verifies the conclusion of Theorem 7.

After the detection of the attack, the new observer proposed in Theorem 8 is applied. As shown in Figure 4.10, the estimated attack magnitude given by the new observer converges to the actual attack magnitude about one second after the attack is launched, which agrees with the conclusion of Theorem 8.

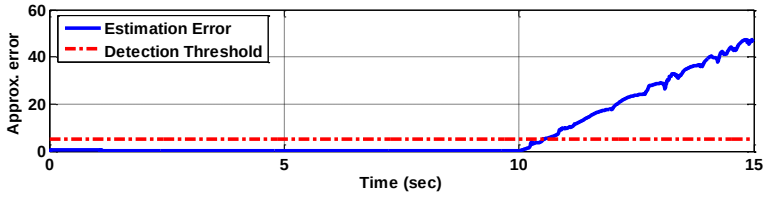


Figure 4.9. Attack detection results for the physical system.

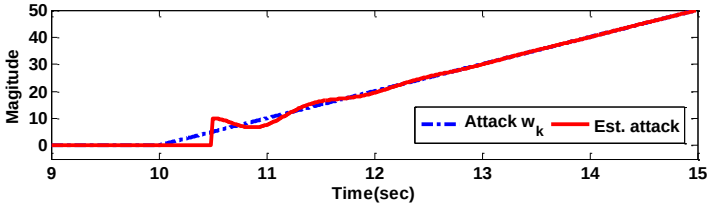


Figure 4.10. Attack estimation of the physical system.

5. CONCLUSIONS AND FUTURE WORK

The presence of communication links to transmit sensor data and control commands has brought in vulnerabilities into NCS. A corrupted communication link can introduce large delays and packet losses, which could lead to the instability of the physical system. This paper proposes a novel cyber-attack detection scheme that is capable of capturing the abnormality in those communication links. The detection of the attacks is faster than the traditional approach where one has to wait for the physical states to be deteriorated. To reduce the data transmissions, an optimal event-trigger control scheme with the presence of network delays and packet losses are revisited. However, the proposed scheme is applicable only to those network attacks causing delays and packets losses while revealing limitation to sophisticated attacks.

6. REFERENCES

[1] C. Yang, Z. Guan, and J. Huang, "Stochastic switched controller design of networked control systems with a random long delay," Asian Journal of Control, vol. 13, no. 2, pp. 255–264, 2011.

[2] P. Lee, C. Andrew, L. Bushnell, and R. Poovendran. "Modeling and designing network defense against control channel jamming attacks: A passivity-based approach," In Control of Cyber-Physical Systems, pp. 161-175. Springer International Publishing, 2013.

[3] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson. "A secure control framework for resource-limited adversaries," Automatica, vol. 51, pp. 135-148, 2015.

[4] H. Sandberg, S. Amin, and K. H. Johansson. "Cyber-physical security in networked control systems: an introduction to the issue," IEEE Control Systems, vol. 35, no. 1, pp. 20-23, 2015.

[5] H. Xu, S. Jagannathan, and F. L. Lewis, "Stochastic optimal control of unknown linear networked control system in the presence of random delays and packet losses," Automatica vol. 48, no. 6, pp. 1017-1030, 2012.

[6] H. Baumman and W. Sandmann, "Markovian modeling and security measure analysis for networks under flooding DoS attacks," 20th Euromicro International Conferences on the Parallel, Distributed and Network-based Processing, pp. 298-302, March 2012.

[7] H. Baumman and W. Sandmann, "Markovian modeling and security measure analysis for networks under flooding DoS attacks," 20th Euromicro International Conferences on the Parallel, Distributed and Network-based Processing, pp. 298-302, March 2012.

[8] Q. Zhu and T. Basar, "Robust and resilient control design for cyber-physical systems with an application to power systems," 50th IEEE Conference on Decision and Control and European Control Conference, pp. 4066-4071, December 2011.

[9] K. Sallhammar, B.E. Helvik, and S.J. Knapskog, "Towards a stochastic model for integrated security and dependability evaluation," IEEE Conference on Availability, reliability and Security, pp. 1-8, September 2006.

[10] A. Cardenas, S. Amin, Z. Lin, Y. Huang, C. Huang, and S. Sastry, "Attacks against process control systems: risk assessment, detection, and response," Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, pp. 355-366, 2011.

[11] L. Liu, M., Esmalifalak, Q. Ding, V. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," IEEE Transaction on Smart Grid, vol. 5, no. 2, pp. 612-621, 2014.

[12] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," IEEE Transactions on Automatic Control, vol. 59, no. 6, pp. 1454-1467, 2014.

[13] Y. Mo and B. Sinopoli, "Integrity attacks on cyber-physical systems," In Proceedings of the 1st international conference on High Confidence Networked Systems, pp. 47-54. ACM, 2012.

[14] H. Niu and S. Jagannathan, Optimal defense and control of dynamic systems modeled as cyber-physical systems, Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, vol. 12, no. 4, pp. 423-438, 2015.

[15] C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," American Control Conference (ACC), pp. 3344-3349, June 2013.

[16] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. Sastry, "Cyber security analysis of state estimators in electric power systems," IEEE Conference on Decision Control, pp. 5991-5998, December 2010.

[17] S. Amin, A. Cárdenas, and S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," Hybrid System Computer Control, vol. 5469, pp. 31–45, April 2009.

[18] M. Zhu and S. Martínez, "Stackelberg game analysis of correlated attacks in cyber-physical systems," American Control Conference, pp. 4063-4068, July 2011.

[19] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," IEEE Transaction on Automatic Control, vol. 58, no. 11, pp. 2715-2729, 2013.

[20] H. Niu and S. Jagannathan, Optimal defense and control of dynamic systems modeled as cyber-physical systems, Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, vol. 12, no. 4, pp. 423-438, 2015.

[21] S. Keshav, "A control-theoretic approach to flow control," ACM, vol. 21, no. 4. pp. 3-15, 1991.

[22] E. Altman, B. François, and J. Bolot, "Discrete-Time Analysis of Adaptive Rate Control Mechanisms," In Data Communication Networks and their Performance, pp. 121-140. 1993.

[23] Y. Hou, S. Panwar, and H. Tzeng, “On Generalized Max-Min Rate Allocation and Distributed Convergence Algorithm for Packet Networks,” IEEE Transactions on Parallel and Distributed Systems, vol. 15, no. 5, pp. 401-416, 2004.

[24] J. C. Bolot, “End-to-end packet delay and loss behavior in the Internet,” In ACM SIGCOMM Computer Communication Review, vol. 23, no. 4, pp. 289-298, 1993.

[25] Y. T. Hou, S. S. Panwar, and H. Tzeng, “On generalized max-min rate allocation and distributed convergence algorithm for packet networks,” Parallel and Distributed Systems, IEEE Transactions on 15, no. 5, pp. 401-416, 2014.

[26] E. Altman, and T. Basar, “Optimal rate control for high speed telecommunication networks,” In Decision and Control, Proceedings of the 34th IEEE Conference on, vol. 2, pp. 1389-1394, December 1995.

[27] S. Jagannathan, and J. Talluri, “Predictive congestion control of ATM networks: multiple sources/single buffer scenario,” Automatica, vol. 38, no. 5, pp. 815-820, 2002.

[28] S. Keshav, “A control-theoretic approach to flow control,” ACM, vol. 21, no. 4, pp. 3-15, 1991.

[29] A. Sahoo, H. Xu, and S. Jagannathan, “Adaptive neural network-based event-triggered control of single-input single-output nonlinear discrete-time systems,” IEEE Transactions on Neural Networks and Learning Systems, vol. 27, no. 1, 2016.

[30] K. S. Narendra and A. M. ANnaswamy, Stable Adaptive Systems. New York: Dover Publications, 2005.

SECTION

2. CONCLUSIONS AND FUTURE WORK

In this dissertation, several novel defense methodologies for CPS have been proposed. First, a special type of cyber-physical system, the RFID system, is considered for which a lightweight mutual authentication and ownership management protocol is proposed in order to protect the data confidentiality and integrity. Then considering the fact that the protection of the data confidentiality and integrity is insufficient to guarantee the security in CPS, we then propose a general framework for developing security schemes for CPS wherein the cyber system states affect the physical system and vice versa. After that, we apply this general framework by selecting the traffic flow as the cyber system state vector and a novel attack detection scheme that is capable of capturing the abnormal traffic flow in the communication links due to a class of attacks. Further, we develop the attack detection and estimation scheme for the traffic flow system when the network parameters are unknown. Finally, this attack detection scheme has been further extended to the case where the network traffic flow is modeled as a nonlinear system with unknown system dynamics. Meanwhile, sensor/actuator attack detection schemes are developed for the physical system where the system dynamics are uncertain due to the network-induced delays and packet losses.

2.1. CONCLUSIONS

In the first paper, a new EPC Gen2v2 compatible protocol by using limited cryptographic functionality was presented for mutual authentication and ownership management. This was done by employing the ultra-lightweight permutation operation

and the PRNG function. Such use of a simple operation adds a minimal level of computation and energy consumption while, at the same time, supports the cryptographic goals of the protocol. The protocol was examined both from a security point of view as well as with a hardware implementation. The analysis indicated that the transactions in the protocol do not expose the secret key information nor does the protocol depend on previously used secret keys, thus guaranteeing that replay or disclosure attacks are not possible. The comparison with previous work shows that the proposed protocol not only conforms to the EPC standards, but also satisfies the security requirements. The hardware implementation supports our initial goal of adding security to the existing EPC Gen2v2 based tags such that the system would be secure both in the case of being used by a single owner or in the more practical cases of having multiple owners during the lifetime of a tagged item.

Next, in the second paper, we have proposed a representation that captures the interrelationship between the cyber and physical systems such that the states in the physical system affect the decision made on the cyber systems and vice versa. Based on this representation, the optimal defense and attacks are given to gain the greatest payoff. Since the proposed representation is in a general form, it can be used in a variety of applications including autonomous systems. In particular, the cyber defender is able to make thorough decisions by selecting appropriate cyber state vector and output and customizing the payoff function that is of interest.

After that, in the third paper, a novel cyber-attack detection scheme that is capable of capturing the abnormality in the communication links is proposed. The detection of the attacks is faster than the traditional approach where one has to wait for the physical states

to be deteriorated. With the proposed detection scheme, attacks on both the networks and the physical plants can be detected. Upon detection, the physical system can be stabilized by re-configuring the controller gain. However, the proposed scheme is applicable only to those network attacks causing delays and packets losses while revealing limitation to sophisticated attacks.

In the fourth paper, we propose a novel cyber-attack detection scheme that is capable of capturing the vulnerable communication links, which is challenging because the system dynamics are considered unknown. The proposed detection scheme for the physical system is able to detect both sensor and actuator attacks. Moreover, the knowledge of the maximum delays and packet losses that the system can tolerate helps the operator protect the plant from further damages based on the ongoing network condition.

Finally, the fifth paper extends the previous work to the case where the network flow dynamics are modeled as a nonlinear system with unknown dynamics. The detection of the attacks is faster than the traditional approach where one has to wait for the physical states to be deteriorated. To reduce the data transmissions, an optimal event-trigger control scheme with the presence of network delays and packet losses are revisited. A sensor/actuator attack detection scheme is developed where the physical system dynamics are uncertain due to the network-induced delays and packet losses. However, the proposed scheme is applicable only to those network attacks causing delays and packets losses while revealing limitation to sophisticated attacks.

2.2. FUTURE WORK

As part of the future work, the proposed general framework in Paper II for the security scheme development can be refined by studying the impact of different attacks on

the network performance to generate a more accurate model for the cyber system dynamics. Furthermore, the adversary model needs not only to be accurate, but also realistic that can reflect the behavior of the attacker in the real world rather than the imagined opponent in the simulation.

Moreover, the proposed attack detection schemes proposed in Papers III through V are applicable only to those network attacks causing delays and packets losses while revealing limitation to sophisticated attacks. In many occasions, as a matter of fact, the adversaries are more intelligent than the defenders. These attackers could learn from the past and know how to maximize the damage while protecting them from being detected. Dealing with sophisticated attacks remains part of the future work.

3. REFERENCES

[1] Y. Zhou and J. Baras, "CPS modeling integration hub and design space exploration with application to microrobotics," In Control of Cyber-Physical Systems, pp. 23-42. Springer International Publishing, 2013.

[2] R. Poovendran, "Cyber–physical systems: close encounters between two parallel worlds," Proceedings of IEEE, vol. 98, no. 8, pp. 1363-1366, 2010.

[3] V. Gunes1, S. Peter1, T. Givargis1, and F. Vahid, "A survey on concepts, applications, and challenges in cyber-physical systems," KSII Transactions on Internet and Information Systems vol. 8, no. 12, pp. 4242-4268, Dec. 2014.

[4] E. Lee, "Cyber physical systems: Design challenges," In Object Oriented Real-Time Distributed Computing (ISORC), 11th IEEE International Symposium on, pp. 363-369, 2008.

[5] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," Automatica, vol. 51, pp. 135-148, 2015.

[6] H. Sandberg, S. Amin, and K. H. Johansson, "Cyber-physical security in networked control systems: an introduction to the issue," IEEE Control Systems, vol. 35, no. 1, pp. 20-23, 2015.

[7] A. Juels, "RFID security and privacy: A research survey," IEEE Journal on Selected Areas in Commun, vol. 24, no. 2, pp. 381-394, Feb. 2006.

[8] P. Lee, A. Clark, L. Bushnell, and R. Poovendran, "A passivity framework for modeling and mitigating wormhole attacks on networked control systems," Automatic Control, IEEE Transactions on 59, no. 12, pp. 3224-3237, 2014.

[9] Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of jamming attacks in time-critical wireless applications," Mobile Computing, IEEE Transactions on 13, no. 8, pp. 1746-1759, 2014.

[10] M, Zhu, and S. Martinez, "On the performance analysis of resilient networked control systems under replay attacks," Automatic Control, IEEE Transactions on 59, no. 3, pp. 804-808, 2014.

[11] N. Falliere, L. O. Murchu, and E. Chien, W32.Stuxnet Dossier Symantec Corporation, 2011.

[12] H. Baumman and W. Sandmann, "Markovian modeling and security measure analysis for networks under flooding DoS attacks," 20th Euromicro International Conferences on the Parallel, Distributed and Network-based Processing, pp. 298-302, March 2012.

[13] Q. Zhu and T. Basar, "Robust and resilient control design for cyber-physical systems with an application to power systems," 50th IEEE Conference on Decision and Control and European Control Conference, pp. 4066-4071, December 2011.

[14] C.W. Ten, G. Manimaran, and C.C. Liu, "Cybersecurity for critical infrastructures: attack and defense modeling," IEEE Transactions on Systems, Management, and Cybernetics, vol. 40, no. 4, pp. 853-865, July 2010.

[15] K. Sallhammar, B.E. Helvik, and S.J. Knapskog, "Towards a stochastic model for integrated security and dependability evaluation," IEEE Conference on Availability, reliability and Security, pp. 1-8, September 2006.

[16] D. Browning, "Flow control in high-speed communication networks," Communications, IEEE Transactions on 42, no. 7 pp. 2480-2489, 1994.

[17] C. Li, and E. Modiano, "Receiver-based flow control for networks in overload," Networking, IEEE/ACM Transactions on 23, no. 2, pp. 616-630, 2015.

[18] J. Jin, W. Wang, and M. Palaniswami, "A simple framework of utility max-min flow control using sliding mode approach," Communications Letters, IEEE 13, no. 5, pp. 360-362, 2009.

[19] A. Aenes, K. Salhammar, K. Haslum, T. Brekne, M. Moe, and S. J. Knapskog, "Realtime risk assessment with network sensors and intrusion detection systems," International Conference on Computational Intellengence and Security, pp. 388-397, December 2005.

[20] C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," American Control Conference (ACC), pp. 3344-3349, June 2013.

[21] L. Liu, M., Esmalifalak, Q. Ding, V. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," IEEE Transaction on Smart Grid, vol. 5, no. 2, pp. 612-621, 2014.

[22] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. Sastry, "Cyber security analysis of state estimators in electric power systems," IEEE Conference on Decision Control, pp. 5991-5998, December 2010.

[23] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," IEEE Transactions on Automatic Control, vol. 59, no. 6, pp. 1454-1467, 2014.

[24] H. Xu, S. Jagannathan, and F. L. Lewis, “Stochastic optimal control of unknown linear networked control system in the presence of random delays and packet losses,” Automatica vol. 48, no. 6, pp. 1017-1030, 2012.

VITA

Haifeng Niu was born on June 14th, 1989, in Tengzhou, Shandong Province, China. He received the Bachelor's degree in Electrical Engineering from Northeastern University, Shenyang, China, in 2010. He was a master student from 2010 to 2012 in Department of Control and Engineering in Zhejiang University, Hangzhou, China. He received his PhD in July 2016 in Department of Electrical Engineering, at Missouri University of Science and Technology under supervision of Professors Jagannathan Sarangapani.

His research interests include adaptive control theorems, RFID networks, wireless networking security, and control-theoretic approach for security of cyber-physical systems.