2016

A Frequency Hopping Method to Detect Replay Attacks

Guofu Tang
Louisiana State University and Agricultural and Mechanical College, gtang3@lsu.edu

A FREQUENCY HOPPING METHOD TO DETECT REPLAY ATTACKS

A Thesis

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Master of Science in Electrical Engineering

in

The Division of Electrical and Computer Engineering

by
Guofu Tang
B.S. in Engineering, Taiyuan University of Technology, 2009
M.S. in Control Theory and Control Engineering, Beijing Jiaotong University, 2013
May 2017

ACKNOWLEDGEMENTS

I would like to express my sincere appreciation to my advisor Dr. Gu Guoxiang for his valuable academic suggestions and patient guidance throughout the research and preparation of this thesis. His expertise and technical advice deeply influenced me and my work recorded herein. Without his valuable suggestions and constructive direction, this thesis would not have been completed.

I would like to appreciate my co-advisor Dr. Zhou Xiangwei for his generous help and patient guidance in my graduate studies. I would also like to thank Dr. Zhou Kemin for serving as the committee.

Thanks also go to my cherished parents and wife who always trust and support me through the years. Without their support, I would not have been able to study here and chase my dream. I deeply thank them.

Finally, I would like to thank all the members in Division of Electrical and Computer Engineering, School of Electrical Engineering and Computer Science (EECS) at Louisiana State University for all the help I received.

TABLE OF CONTENTS

ABSTRACT

The application of information technology in network control systems introduces the potential threats to the future industrial control system. The malicious attacks undermine the security of network control system, which could cause a huge economic loss. This thesis studies a particular cyber attack called the replay attack, which is motivated by the Stuxnet worm allegedly used against the nuclear facilities in Iran. For replay attack, this thesis injects the narrow-band signal into control signal and adopts the spectrum estimation approach to test the estimation residue. In order to protect the information of the injected signal from knowing by attackers, the frequency hopping technology is employed to encrypt the frequency of the narrow-band signal. The detection method proposed in the thesis is illustrated and examined by the simulation studies, and it shows the good detection rate and security.

CHAPTER 1
INTRODUCTION

As evidenced in the past two decades, the information technology (IT) such as wireless and networking technologies have been making profound impacts not only on our daily life but also on various engineering branches. In particular networked control systems (NCS) are made possible in which the physical system and feedback controller are situated in two different locations and connected through wireless networks. The new development of the NCS is important as often robots and other controlled systems have to work in hazardous environments where wired connection is not allowed or prohibited. Moreover, the NCS often shares communication channels with other users, which improves the efficiency of communication. The block diagram in Figure 1.1 illustrates schematically the structure of the NCS.

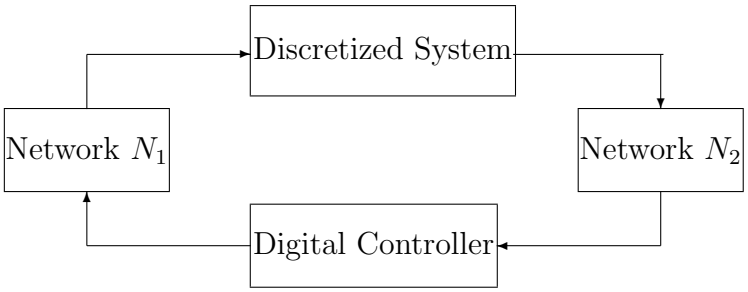

Figure 1.1: Networked control system (NCS)

The NCS overturns the traditional structure of the control system that is a point-to-point single loop control strategy, and allows multiple physical plants, controllers, actuators and sensors to be integrated into a system of systems. This new structure helps control systems to be adapted to the development of science and technology. It makes possible to integrate a large number of nodes distributed in a large area into a large system, such as mobile sensor networks [1], multi-agent systems [2], and automated highway systems [3] etc. In the near future, the NCS can even be implemented through the internet so that control systems can be distributed around the world. Furthermore, the NCS can reduce the cost, and is easy

to maintain. Hence the NCS can be widely deployed in the industry, agriculture, military defense, and out-space exploitation.

In the past decade, researchers in the control community have mainly focused their research on packet loss, time delay, and synchronization problems of the NCS. However the development of the NCS also gives rise to the security problem, due to the use of wireless and networking technologies. Adversaries can launch attacks anywhere and anytime. The security problem of the NCS has attracted great attention from the research community since 2010, especially after the news of the Stuxnet malware was made public. It was allegedly designed to attack Siemens controller known as P.C.S.-7, and caused a huge loss on Iran's nuclear enrichment factories in 2009 [4], [5]. The Stuxnet malware can reside in computer systems and programmable logic controllers (PLCs), and it can migrate from computers to PLCs, and from PLCs to computers without launching attacks until it is populated to a large percentage of computers and PLCs. When the Stuxnet malware finally launches attacks, it replays the past outputs of the PLCs to conceal the actual situation of the control processes from the supervisory control and data acquisition (SCADA) system. Hence often the SCADA fails to detect the replay attacks, and the results of the attack can be catastrophic. Since the PLCs are widely used in the industrial control processes around the world, and Stuxnet malware has since spread to many window-based computer systems, it becomes a very urgent research problem for engineers and researches to develop new approaches and methods to detect the replay attacks, and protect the industrial control systems.

1.1 Overview of the Existing Work

In the past several years, quite a few researchers ([6], [7], [8], [9], [10], and [11]) have paid great attention to the replay attack in the NCS, motivated by the Stuxnet malware. An overview of the existing work will be provided as follows.

Mo and Sinopoli are the first to study the replay attack in the NCS [6]. They assume that the physical system is a discrete time linear time invariant system, and the feedback controller

is designed based on the infinite horizon Linear Quadratic Gaussian (LQG) method. The simplest replay attack is considered in [6]: the replay attacker first hijacks the sensors and records secretly the system output for certain period of time; when the attack is launched, the past readings of the output data are replayed to the feedback controller so that the attacks to the physical system can be hidden from being detected until it is too late. It is observed by Mo and Sinopoli that the LQG controller uses the control input

$$u(t) = u_*(t) = F\hat{x}(t|t-1), \tag{1.1}$$

where t is integer valued, F is the controller gain, and $\hat{x}(t|t-1)$ is the optimal estimation of the system state of time t based on the output measurements up to time $t-1$. Since the LQG controller is the Kalman filter that is the optimal one-step predictor, the control signal $u_*(t)$ is readily available. Assuming that the system output is given by $y(t) = Cx(t) + v(t)$ with $x(t)$ the system state and $v(t)$ is white Gauss distributed, the output estimation error

$$\delta y(t) = y(t) - C\hat{x}(t|t-1)$$

is also white and Gauss distributed. As a result, $\|\delta y(t)\|^2$ has a χ^2 distribution. For this reason, Mo and Sinopoli proposes to use the χ^2 failure detector to detect the reply attack, i.e., the detector is described by the following equation:

$$g_t = \sum_{k=t-N+1}^{t} \left[y(k) - C\hat{x}(k|k-1)\right]' \mathbb{P}^{-1} \left[y(k) - C\hat{x}(k|k-1)\right] \lesseqgtr \text{threshold}, \tag{1.2}$$

where C is the system output matrix, N is the detection window, and $\mathbb{P}$ is the covariance of $\delta y(t) = y_t - C\hat{x}_{t|t-1}$. If the plant model is stable, then the output estimation error $\delta y(t)$ remains the same as pointed in [6], due to the fact that the attacker feedbacks the system output in the distant past. Consequently χ^2 failure detector fails to detect the replay attack. Therefore Mo and Sinopoli propose to inject an independent identically distributed (i.i.d.)

zero-mean Gaussian noises, denoted as $_{\triangle}u$ into the control input. Roughly speaking the injected white Gauss noises are the authentication signal that serve as the time stamp. The Kalman filter knows the injected Gauss white noises, and thus $\delta y(t)$ remains the same when the replay attacks are absent. However the injected Gauss white noises cannot be canceled by the Kalman filter, if the adversaries launch the replay attack, and thus the χ^2 failure detector can successfully detect the replay attack. In addition [6] provides the quantitative analysis on the relationship between the control system performance and the the variance of the injected authentication signal, and the relationship between the detection rate and the variance of injected authentication signal.

The work of [6] motivates others to follow. Because the injected white Gauss authentication signal degrades the control system performance, Thien-Toan Tran, Oh-Soon Shin, and Jong-Ho Lee proposes a modification in [9] in studying the replay attack detection problem in smart grid systems. In order to protect the customer equipment and obtain the accurate power usage data from the smart meters, they propose to modify the original solution in [6] so that it can efficiently detect replay attacks without increasing the burden to the system. Specifically, they inject the authentication random signal $_{\triangle}u$ periodically and keep it on for a certain time duration and set it off for another certain time duration within each period. By carefully adjusting the portion of the period to add the authentication signal, the negative impact to the system is reduced while χ^2 failure detector can still retain its sufficient detection capability.

Fei Miao, Miroslav Pajic, and George J. Pappas propose a method in [10] to tradeoff the control system performance and the detection rate for replay attack from another standpoint of view. They believe that the competitive relationship between the attacker and the control system can be described as a noncooperative game model. The outline of their paper can be summarized as following.

The authors assume that both the control system and the replay attacker are able to observe the state of the game, but none of them has the exact previous behavior information

of the other. The game is assumed to work in three modes: safe, no detection, and false alarm trigger. According to the state transition probability and the attacker's action space, the optimal switching control policy can be obtain to minimize the worst case control and detection cost. The controller will shift between control cost optimal mode and the secure mode as shown in Figure 1.2. By utilizing the suboptimal algorithm based on the value iteration method for finite horizon stationary stochastic game, they obtain the optimal control strategy at each stage.

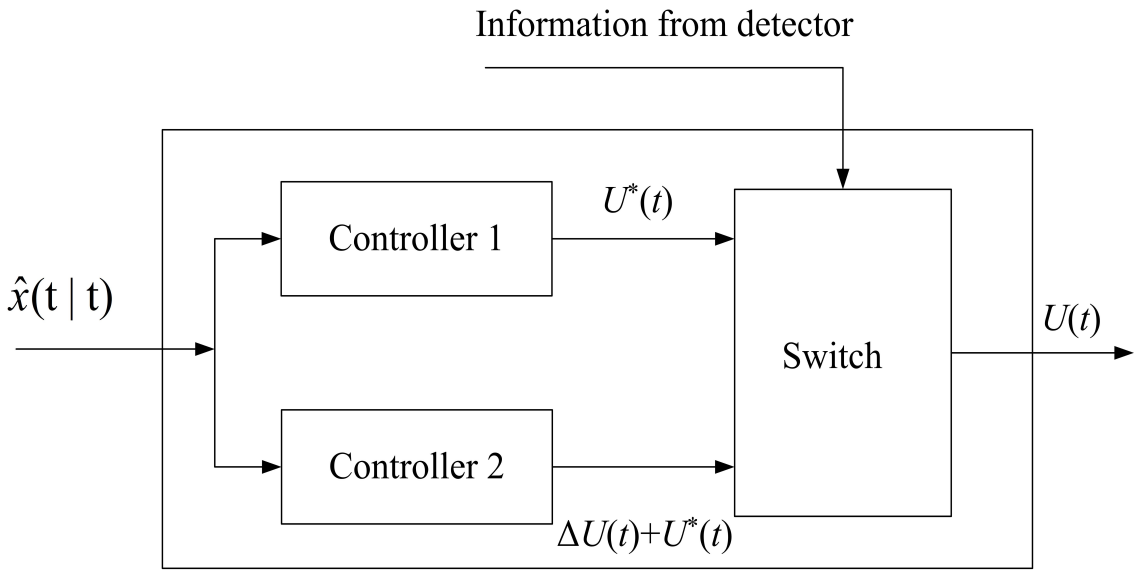

Figure 1.2: The diagram of the switching controller

Due to the added authentication signal degrade the control system performance, Bixiang Tang, Luis D. Alvergue, and Guoxiang Gu consider the method without injecting any authentication signal into control input to detect the replay attack in [11]. They assume that the communication channel is additive white Gaussian noise (AWGN), and the output addictive noise $\eta(t)$ is composed of the measurement noise $\eta_o(t)$ and the communication error $\eta_c(t)$. A whitening filter is designed to convert the input and output signals into white signal

$w(t)$. When the replay attack takes place, the PSD of the controller input $w(t)$ will not be white anymore. Because the falsified feedback signal adds the communication error up, which changes the PSD of the feedback signal at some frequency ω_h at which the controller has a high gain. In the absent of the replay attack, the PSD of $w(t)$ is

$$\Phi_w(\omega_h) = \delta_d^2 V(e^{j\omega_h}) V(e^{j\omega_h})^*, \tag{1.3}$$

In the presence of the replay attack, the PSD of $w(t)$ is

$$\Phi_w(\omega_h) = \delta_d^2 V(e^{j\omega_h}) V(e^{j\omega_h})^* + 2\delta_{\eta_c}^2 I_m, \tag{1.4}$$

where $V(z)$ is related to the whitening filter, and δ_d^2 depends on the variance of the process and measurement noises, while $\delta_{\eta_c}^2$ represents the channel noise variance. The PSD detector can be constructed as

$$\Phi_w(\omega_h) \gtrless \text{threshold}. \tag{1.5}$$

By utilizing the communication error, the proposed method in [11] does not need to inject the authentication signal into the control system while being capable of detecting the replay attack. Hence this method does not degrade the control system performance. More importantly this method works for non-LQG control systems, and hence has more applicability compared to other known methods.

1.2 Thesis Contribution

As discussed in the previous section, Mo and Sinopoli [6] are the first to study the replay attack in the LQG based NCS, and proposed a method to tackle the detection of the replay attack. By injecting the white Gaussian authentication signal with suitable large variance into the control input, the replay attack can be detected by the χ^2 failure detector by testing the output estimation error that is white and Gauss distributed due to the use of the

Kalman filter in the LQG controller. However the control system performance is degraded by the injected authentication signal with large variance. Authors of [9] try to tradeoff the control system performance and the detection rate by periodically injecting the white Gauss authentication signal. It reduces the negative impact of the injected signal on control system, but the detection time depends on the frequency of the injected signal. Moreover this method can cause large time delay in detecting replay attacks due to the periodic absence of the injected authentication signal. The results in [11] present an ideal method to detect replay attack without injecting any authentication signal into control input. However this ideal method is based on a very strong assumption that the communication channel of the NCS is white addictive Gaussian channel. Otherwise the method proposed in [11] will not work. Although [10] proposes another way to study the detection problem of the replay attack, it does not balance well the control system performance and the detection rate. The reason lies in the fact that the method based on the noncooperative game theory cannot provide accurate prediction of the replay attack, which determines the switching between the LQG controller and the secure controller (with injected authentication Gauss signal). As a result it causes degradation of the control system performance seriously or induces large delay in detecting the attacks.

The inadequacies of the existing detection methods motivate us to continue investigation for detection of the replay attack, and to develop new methods and new ideas in order to improve the existing detection method. The contribution of this thesis is summarized next.

- We propose to inject narrow-band authentication signal in the control input, contrasting to the white Gaussian noises used in the known work. Specifically pure sinusoidal signals are injected to the control input which clearly have narrow-band. As a result spectrum estimation methods can be used to detect the replay attack. Because the PSD of this narrow-band signal concentrates at certain frequency, it is possible to inject the authentication signal with large variance while keeping the minimum negative impact to the control system performance.

- In our studies, we discover the replay attacker can evade the detection by launching a smart attack strategy, if the frequency of the injected signal is known by the attacks who may have the capability to estimate the frequency of the narrow-band authentication signal. So we propose to employ the frequency hopping detection method to encrypt the frequency of the injected signal. This way helps to protect the spectrum information of the authentication signal from being estimated by attackers. Although the randomly shifting frequency affects the detection rate to some extend, the frequency hopping method still shows the high detection rate if large detection window size is used.

- Simulation studies are carried out for detection of the replay attacks. First the known method based on white Gaussian authentication signals is studied using numerical simulations. Second the spectrum detection method based on our proposed narrow-band authentication signals is also studied in numerical simulations. The results are compared, and conclusions are drawn, which show the superiority of the spectrum detection method.

1.3 Organization of the thesis

The mathematical notation is standard, and will be made clear in later chapters. This section outlines organization of the thesis.

- Chapter 1 provides the overview of the existing work, and the contribution of this thesis.

- In Chapter 2, we introduce the background material, including knowledge on systems and signals. For signals, sinusoidal functions and their PSDs are used to illustrate random processes. For systems, state space descriptions are employed. This chapter also covers the stability of finite dimensional linear time-invariant systems.

- In Chapter 3, we cover the LQG controller and Kalman filter. The LQG controller is composed of two parts: one is the optimal state feedback controller, and the other is

the optimal state estimator. Assuming that the system states are measurable, then we can obtain the optimal state feedback controller. When the system states are not measurable and the process and measurement noises are all white and Gauss distributed, then the optimal state estimator, that is the Kalman filter, can be employed to obtain the optimal state estimation. The use of the estimated state and the Kalman filter in the optimal state feedback controller constitutes the LQG controller. The whiteness property of the output estimation error is highlighted.

- In Chapter 4, the white noise method proposed in [6] is studied first. We then investigate the spectrum method by injecting the narrow-band authentication signal in the control input to detect the replay attack. Because the spectrum detection method can fail when the replay attacker knows the characteristics such as angular frequency of the injected authentication signal, we propose to employ the frequency hopping communication technology to encrypt the frequency of the narrow-band signal. The simulation results show that the performance of the frequency hopping detection method is better than that of the white noise method under the same condition.

- Chapter 5 concludes the thesis by summarizing the research work and by outlining the possible directions for future studies.

CHAPTER 2
BACKGROUND MATERIAL

This chapter provides the background material of this thesis, including random signals, power spectrum density, and state space description for linear time-invariant systems. All signals and systems are in discrete-time with t for time index.

2.1 Signals and Systems

Signals can be mainly divided into two categories: one is the determinist signal, and the other is the random signal. We will focus on vector-valued random signals in this paper.

For a vector signal $s(t)$, its autocorrelation sequence (ACS) is defined by

$$R_s(k,t) := \mathrm{E}\left\{s(t)s(t-k)^*\right\}, \quad k = 0, \pm 1, \pm 2, \cdots \tag{2.1}$$

which is a square matrix and depends on both t and k in general. If $R_s(k) = R_s(k,t)$ is independent of t, then $s(t)$ is said to be wide-sense stationary (WSS). In this case, the power spectral density (PSD) of $s(t)$ is defined by

$$\Phi_s(\omega) = \sum_{k=-\infty}^{\infty} R_s(k) e^{-jk\omega}, \tag{2.2}$$

that is the discrete-time Fourier transform (DTFT) of $s(t)$. The mean power of $s(t)$ is $P_s = \mathrm{E}\{\|s(t)\|^2\}$, and the power norm of $s(t)$ is defined by

$$\|s\|_{\mathbb{P}} := \sqrt{P_s} = \sqrt{\mathrm{E}\{\|s(t)\|^2\}} = \sqrt{\mathrm{T_r}\{R_s(0)\}}. \tag{2.3}$$

The following is an example of a WSS random signal.

Example 1. *Consider a random signal*

$$s(t) = A\cos(\omega_0 t + \Theta), \quad 0 < \omega_0 < 2\pi,$$

where ω_0 is real constant, A and Θ are real random variables, independent to each other, and uniformly distributed over $[0,1]$ and $[0,2\pi)$, respectively. The mean value of the signal can be easily computed as follows:

$$\begin{aligned} \mathrm{E}\{s(t)\} &= \mathrm{E}\{A\cos(\omega_0 t+\Theta)\} \\ &= \mathrm{E}\{A\}\mathrm{E}\{\cos(\Theta)\}\cos(\omega_0 t) - \mathrm{E}\{A\}\mathrm{E}\{\sin(\Theta)\}\cos(\omega_0 t) = 0 \end{aligned} \tag{2.4}$$

by independence of A and Θ, and $\mathrm{E}\{\cos(\Theta)\} = \mathrm{E}\{\sin(\Theta)\} = 0$. The ACS of the signal can be obtained by straightforward calculation:

$$\begin{aligned} \mathrm{E}\{s(t)\bar{s}(t-k)\} &= \mathrm{E}\{A^2\cos(\omega_0 t+\Theta)\cos(\omega_0(t-k)+\Theta)\} \\ &= \tfrac{1}{2}\mathrm{E}\{A^2\}\mathrm{E}\{\cos(\omega_0 k) + \cos(2\omega_0 t - \omega_0 k + 2\Theta)\} \\ &= \tfrac{1}{2}\mathrm{E}\{A^2\}\cos(\omega_0 k) = \tfrac{1}{6}\cos(\omega_0 k) =: r_s(k), \end{aligned} \tag{2.5}$$

that is independent of time index t. Hence $s(t)$ is a WSS process.

A linear time-invariant system (LTI) can be considered as a map that maps the system input to the system output as shown in Figure 2.1.

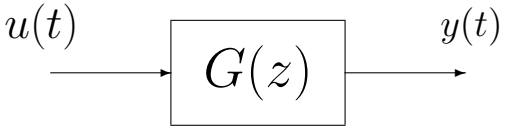

Figure 2.1: The LTI system

Let $g(t)$ be the impulse response, the transfer function of the system in Figure 2.1 is the Z-transform of its impulse response:

$$G(z) = \sum_{t=-\infty}^{\infty} g(t)z^{-t}, \quad z \in \mathbb{C}. \tag{2.6}$$

The LTI system in Figure 2.1 is assumed to be bound-input and bound-output (BIBO) stable. Furthermore, the functional relationship of the system input and output is given by the convolution:

$$y(t) = g(t) * u(t) = \sum_{t=-\infty}^{\infty} g(t-k)u(k). \tag{2.7}$$

If the input $u(t)$ is a WSS signal, then the output $y(t)$ is also a WSS signal in steady-state. More importantly, the PSD of the output is related to the PSD of the input according to the following mathematical relation:

$$\Phi_y(\omega) = G(e^{j\omega})\Phi_u(\omega)G(e^{j\omega})^* \tag{2.8}$$

Let the input signal $u(t)$ be white process with mean zero and covariance identity. Then the output mean power is obtained as

$$P_y = \mathrm{E}\left\{\|y(t)\|^2\right\} = \mathrm{Tr}\left[\mathrm{E}\left\{R_y(0)\right\}\right] = \mathrm{Tr}\left\{\frac{1}{2\pi}\int_{-\pi}^{\pi} G(e^{j\omega})G(e^{j\omega})^* d\omega\right\} \tag{2.9}$$

by the fact that $\Phi_u(\omega) = I \ \forall \ \omega$. The above introduces the $\mathcal{H}_2$ norm of $G(z)$:

$$\|G\|_2 = \sqrt{\mathrm{Tr}\left\{\frac{1}{2\pi}\int_{-\pi}^{\pi} G(e^{j\omega})G(e^{j\omega})^* d\omega\right\}} = \sqrt{\mathrm{Tr}\left\{\sum_{t=-\infty}^{\infty} g(t)g(t)^*\right\}} \tag{2.10}$$

2.2 State Space Descriptions

If every entry of $G(z)$ in Figure 2.1 is a rational function of z, then it can be described by state-space equations:

$$x(t+1) = Ax(t) + Bu(t), \qquad x(0) = x_0, \tag{2.11a}$$

$$y(t) = Cx(t) + Du(t), \tag{2.11b}$$

where (A, B, C, D) is a realization of the system with transfer matrix $G(z)$, and $x(t) \in \mathbb{R}^n$ is the state vector, $u(t) \in \mathbb{R}^m$ is the input, and $y(t) \in \mathbb{R}^p$ is the output. It follows that

$$A \in \mathbb{R}^{n\times n}, \qquad B \in \mathbb{R}^{n\times m}, \qquad C \in \mathbb{R}^{p\times n}, \qquad D \in \mathbb{R}^{p\times m}.$$

Recall that $G(z)$ is the transfer matrix of system, which admits state-space description (2.11). We denote

$$G(z) = \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right] := D + C(zI - A)^{-1}B. \tag{2.12}$$

For the above system described in (2.11), (A, B) is said to be controllable, if

$$\text{rank}\left\{\left[\begin{array}{cccc} B & AB & \cdots & A^{n-1}B \end{array}\right]\right\} = n. \tag{2.13}$$

Similarly (C, A) is said to be observable, if

$$\text{rank}\left\{\left[\begin{array}{c} C \\ CA \\ \cdots \\ CA^{n-1} \end{array}\right]\right\} = n. \tag{2.14}$$

In addition, (A, B) is said to be stabilizable, if

$$\text{rank}\left\{\left[\begin{array}{cc} A - \lambda I, & B \end{array}\right]\right\} = n, \quad \forall |\lambda| \geq 1. \tag{2.15}$$

The above is equivalent to that if $x^*A = \lambda x^*$ satisfying

$$x \in \mathbb{R}^n, \quad x^* \neq 0, \quad \text{and} \quad |\lambda| \geq 1,$$

then there holds $x^*B \neq 0$. Similarly (C, A) is said to be detectable, if

$$\text{rank}\left\{\left[\begin{array}{c} A - \lambda I \\ C \end{array}\right]\right\} = n, \quad \forall |\lambda| \geq 1. \tag{2.16}$$

Equivalently if $Ax = \lambda x$ satisfying

$$x \in \mathbb{R}^n, \quad x \neq 0, \quad \text{and} \quad |\lambda| \geq 1,$$

then there holds $Cx \neq 0$.

The state space system described in (2.11) is said to be internally stable, if all eigenvalues of A lie strictly inside the unit circle. Considering the linear system described by (2.11), the following results is well known [12]:

Theorem 1. *The system described by* (2.11) *is said to be internally stable, if and only if for any given* $Q = Q' > 0$*, there exists a positive definite solution* X *to*

$$X = AXA' + Q. \tag{2.17}$$

If (A, B) *is controllable, then the system described in* (2.11) *is internally stable, if and only if there exists a positive definite solution* X *to the Lyapunov equation*

$$X = AXA' + BB'. \tag{2.18}$$

If (A, B) *is stabilizable, then the system described in* (2.11) *is internally stable, if and only if there exists a positive semi-definite solution* X *to* (2.18)*.*

Performance optimization is a central objective in feedback system design in addition to feedback stability. An important performance measure for feedback control systems is disturbance rejection. Its general formulation is schematically illustrated in the next page.

In Figure 2.2, $d(t) \in \mathbb{R}^{m_1}$ is the disturbance input and $u(t) \in \mathbb{R}^{m_2}$ is the control input, while $\omega(t) \in \mathbb{R}^{p_1}$ is the output signal to be controlled and $y(t) \in \mathbb{R}^{p_2}$ is measured output. The transfer matrix from $\{d(t), u(t)\}$ to $\{w(t), y(t)\}$ is given by

$$G(z) = \left[\begin{array}{c|cc} A & B_1 & B_2 \\ \hline C_1 & D_{11} & D_{12} \\ C_2 & D_{21} & D_{22} \end{array}\right] \tag{2.19}$$

where $G_{ij}(z) = D_{ij} + C_i(zI - A)^{-1}B_j$ for $i, j = 1, 2$ and $A \in \mathbb{R}^{n\times n}$. The transfer matrix $K(z)$ represents the feedback controller. Hence the closed-loop transfer matrix from disturbance

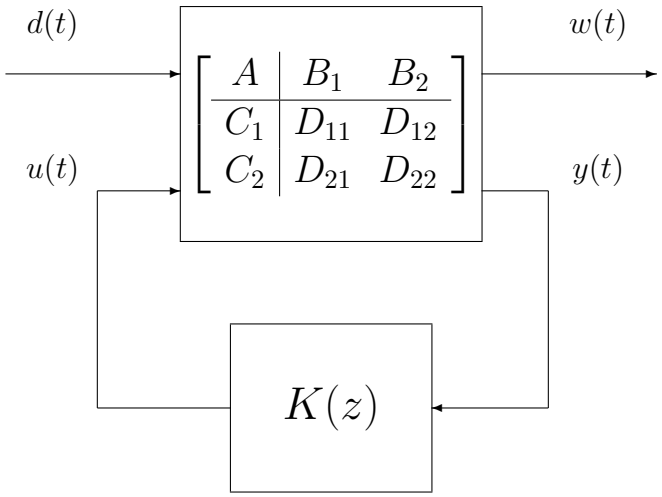

Figure 2.2: LTI feedback control system

input $d(t)$ to system controlled output $w(t)$ is obtained as

$$T_{d\omega}(z) = G_{11}(z) + G_{12}(z)K(z)[I - G_{22}(z)K(z)]^{-1}G_{21}(z) =: \mathcal{F}_\ell[G(z), K(z)]$$

that is the lower linear fractional transform (LFT). Minimization of the power norm of $w(t)$ is equivalent to minimization of the $\mathcal{H}_2$ norm of $T_{dw}(z)$, subject to the feedback stability, which is referred to as $\mathcal{H}_2$ control. If in addition, $K(z)$ is required to be strictly proper in minimizing the $\mathcal{H}_2$ norm of $T_{dw}(z)$, then this is called linear quadratic Gauss (LQG) control. We will be more specific in the next chapter.

CHAPTER 3
PROBLEM FORMULATION

Recall the feedback system in Figure 2.2. The state-space model of the generalized plant $G(z)$ is described by

$$x(t+1) = Ax(t) + B_1 d(t) + B_2 u(t), \tag{3.1a}$$

$$w(t) = C_1 x(t) + D_{11} d(t) + D_{12} u(t), \tag{3.1b}$$

$$y(t) = C_2 x(t) + D_{21} d(t) + D_{22} u(t), \tag{3.1c}$$

where $x(t) \in \mathbb{R}^n$ is the state vector, $y(t) \in \mathbb{R}^{p_2}$ is the output vector, $d(t) \in \mathbb{R}^{m_1}$ is the noise vector, $u(t) \in \mathbb{R}^{m_2}$ is the control vector, and $w(t) \in \mathbb{R}^{p_1}$ is the vector to be estimated, both m_2 and p_2 usually are strictly smaller than n.

In this chapter we briefly describe the LQG controller design and Kalman filter design based on which the existing detection strategies to replay attack will be introduced.

3.1 LQG Control

Linear Quadratic Gaussian (LQG) control is aimed at minimizing the variance or mean-power of the controlled signal $w(t)$, in addition to feedback stabilization. It consists of the optimal state feedback control and the optimal state estimation. The optimal controller minimizes mean-power of the controlled signal $w(t)$ based on state feedback control, and the optimal estimator provides the minimum mean-squared error (MMSE) estimation of the system state. Because $\mathcal{H}_2$ is more general, we begin with the design of the $\mathcal{H}_2$ controller before we introduce the LQG control.

Assuming that D_{22} is zero and the system state and external disturbance are known, the $\mathcal{H}_2$ control law will be the full information (FI) controller:

$$u(t) = u_F(t) = Fx(t) + F_0 d(t). \tag{3.2}$$

Recall the system performance index $\mathrm{E}\{\|w(t)\|^2\}$. If the feedback system is internally stable under the FI control, then $w(t)$ is a wide-sense stationary (WSS) process asymptotically and thus $\mathrm{E}\{\|w(t)\|^2\}$ is independent of time t asymptotically. Substituting the FI control law (3.2) in to (3.1a) and (3.1b) yields

$$x(t+1) = (A + B_2F)x(t) + (B_1 + B_2F_0)d(t), \tag{3.3a}$$

$$w(t) = (C_1 + D_{12}F)x(t) + (D_{11} + D_{12}F_0)d(t). \tag{3.3b}$$

Hence the FI controller is required to minimize the $\mathcal{H}_2$-norm of the transfer matrix from the disturbance input $d(t)$ to controlled signal $w(t)$. That is, the FI controller needs to be designed to minimize the $\mathcal{H}_2$-norm of following transfer matrix:

$$T_{dw}(z) = T_{FI}(z) := \left[\begin{array}{c|c} A + B_2F & B_1 + B_2F_0 \\ \hline C_1 + D_{12}F & D_{11} + D_{12}F_0 \end{array}\right]. \tag{3.4}$$

The $\mathcal{H}_2$ solution to minimizing $\|T_{FI}\|_2$ is given by

$$F = -(R + B_2^*XB_2)^{-1}(B_2^*XA + D_{12}^*C_1), \quad R = D_{12}^*D_{12}, \tag{3.5a}$$

$$F_0 = -(R + B_2^*XB_2)^{-1}(B_2^*XB_1 + D_{12}^*D_{11}), \tag{3.5b}$$

where $X \geq 0$ is the stabilizing solution of the algebraic riccati equation (ARE):

$$X = \tilde{A}^*X(I_n + B_2R^{-1}B_2^*X)^{-1}\tilde{A} + C_1^*(I - D_{12}R^{-1}D_{12}^*)C_1, \quad \tilde{A} = A - B_2R^{-1}D_{12}^*C_1. \tag{3.6}$$

Since the system state and external disturbance may not be measured directly in practice, the true system true state and disturbance need to be estimated. The corresponding problem of the output estimation can be described by

$$x(t+1) = Ax(t) + B_1 d(t) + B_2 u(t), \tag{3.7a}$$

$$u(t) = u_{\mathrm{FI}}(t) := Fx(t) + F_0 d(t), \tag{3.7b}$$

$$y(t) = C_2 x(t) + D_{21} d(t). \tag{3.7c}$$

Our goal is to estimate $u_{\mathrm{FI}}(t)$ based on measurements of $y(t)$. In order to obtain the optimal FI estimation, and control law, the MMSE estimator needs to be developed, assuming white Gaussian noise $d(t)$, which has the form:

$$\hat{x}(t+1) = A\hat{x}(t) + L\left[C_2\hat{x}(t) - y(t)\right] + B_2 u(t), \tag{3.8a}$$

$$u(t) = \hat{u}(t) := F\hat{x}(t) + L_0[C_2\hat{x}(t) - y(t)], \tag{3.8b}$$

where L and L_0 are the respective state and disturbance estimation gain of the output estimator. The MMSE estimation (L, L_0) gains are obtained as

$$L = -(AYC_2^* + B_1 D_{21}^*)(\tilde{R} + C_2 Y C_2^*)^{-1}, \tag{3.9a}$$

$$L_0 = -(FYC_2^* + F_0 D_{21}^*)(\tilde{R} + C_2 Y C_2^*)^{-1}, \tag{3.9b}$$

where $\tilde{R} = D_{21}D_{21}^* > 0$ and $Y \geq 0$ is the stabilizing solution to the ARE

$$Y = A_{\tilde{R}} Y (I + C_2^* \tilde{R}^{-1} C_2 Y)^{-1} A_{\tilde{R}}^* + B_1 (I - D_{21}^* \tilde{R}^{-1} D_{21}) B_1^*, \quad A_{\tilde{R}} = A - B_2 D_{21}^* \tilde{R}^{-1} D_{21} C_2. \tag{3.10}$$

Substituting (3.8b) into (3.8a) yields the state description of the optimal $\mathcal{H}_2$ feedback controller described by state space equation

$$\begin{aligned} \hat{x}(t+1) &= (A + B_2F + LC_2 + B_2L_0C_2)\hat{x}(t) - (L + B_2L_0)y(t), \\ u(t) &= (F + L_0C_2)\hat{x}(t) - L_0 y(t) \end{aligned} \tag{3.11}$$

Let $\hat{A}, \hat{B}, \hat{C}, \hat{D}$ be realization of $K(z)$ described in (3.11). If $D_{22} = 0$, then

$$\begin{aligned} \hat{A} &= A + B_2F + LC_2 + B_2L_0C_2, & \hat{B} &= L + B_2L_0, \\ \hat{C} &= F + L_0C_2, & \hat{D} &= L_0. \end{aligned}$$

It is important to note that the estimator in (3.8a) and (3.8b) makes the use of $y(t)$ in estimation of $u_{\mathrm{FI}}(t)$. Hence $K(z) = \hat{D} + \hat{C}(zI - \hat{A})^{-1}\hat{B}$ is called the H_2 controller. If $y(t)$ is not allowed in estimation of $u_{\mathrm{FI}}(t)$, then $L_0 = 0$ can be taken, which is referred to as LQG controller.

3.2 Kalman Filter

In engineering practice, various disturbances are unavoidable in operating systems, which affect adversely to the controlled system outputs. Most these disturbances are white noises with Gauss distribution. Therefore Kalman filter is widely employed in engineering practice for estimation due to its easy installation, fast computation, low storage requirement, and being the MMSE estimation. This section is focused on Kalman filtering.

Consider the more generally time-varying state-space system described by

$$\begin{aligned} x(t+1) &= A_t x(t) + B_t v(t) \\ y(t) &= C_t x(t) + D_t v(t), \end{aligned} \tag{3.12}$$

where A_t, B_t, C_t, D_t are allowed to be time-varying, and $v(t)$ is the random process with Gaussian distribution of zero mean and identity covariance. Let $\hat{x}(t|k)$ be the MMSE estimate of $x(t)$ based on measurements of $y(\cdot)$ up to time k. Then the Kalman filter can be obtained as follow:

$$\hat{x}(t+1|t) = (A_t + K_t C_t)\hat{x}(t|t-1) - K_t y(t), \quad \hat{x}(0|-1) = \bar{x}(0), \tag{3.13a}$$

$$K_t = -A_t \Sigma_t C_t^* (R_t + C_t \Sigma_t C_t^*)^{-1}, \tag{3.13b}$$

$$\Sigma_{t+1} = A_t \Sigma_t A_t^* + B_t B_t^* + K_t C_t \Sigma_t A_t^*, \quad \Sigma_0 = P_0. \tag{3.13c}$$

where$\Sigma_k = \Sigma_{k|k-1}$, and $B_t D_t^* = 0$ and $R_t = D_t D_t^* \geq 0 \, \forall \, t \geq 0$ are assumed. For the case $B_t D_t^* \neq 0$, the above Kalman filter can be replaced by

$$\hat{x}(t+1|t) = (A_t + K_t C_t)\hat{x}(t|t-1) - K_t y(t), \quad \hat{x}(0|-1) = \bar{x}(0), \tag{3.14a}$$

$$K_t = -(A_t \Sigma_t C_t^* + B_t D_t^*)(R_t + C_t \Sigma_t C_t^*)^{-1}, \tag{3.14b}$$

$$\Sigma_{t+1} = \tilde{A}_t (I_n + \Sigma_t C_t^* R_t^{-1} C_t)^{-1} \Sigma_t \tilde{A}_t^* + \tilde{B}_t \tilde{B}_t^*, \quad \Sigma_0 = P_0, \tag{3.14c}$$

where $\tilde{A}_t = A_t - B_t D_t^* R_t^{-1} C_t$ and $\tilde{B}_t = B_t (I - D_t R_t^{-1} D_t)$. The Kalman filter provides an efficient and recursive algorithm for computing the MMSE estimate of the system state. An important property of the Kalman filter is the following:

Proposition 2. *For the Kalman filter described in* (3.13a)- (3.13c)*, the output estimate error* $\delta y(t) = y(t) - \hat{y}(t)$ *is a white process.*

Proof. For convenience, we denote $\hat{x}(t) = \hat{x}(t|t-1)$. Let $\hat{x}_e(t) = x(t) - \hat{x}(t)$ be the state estimation error. Its dynamics are described by

$$\begin{aligned} \hat{x}_e(t+1) &= (A_t + L_t C_t)\hat{x}_e(t) + (B_t + L_t D_t)v(t), \\ \delta y(t) &= C_t \hat{x}_e(t) + D_t v(t), \end{aligned} \tag{3.15}$$

where $\hat{y}(t) = C_t \hat{x}(t)$. The associated error covariance of $\hat{x}_e(t)$ satisfies the following difference Lyapunov equation

$$X_{t+1} = (A_t + L_t C_t) X_t (A_t + L_t C_t)^* + (B_t + L_t D_t)(B_t + L_t D_t)^*, \tag{3.16}$$

by the independent of $\hat{x}_e(t)$ and $v(t)$. In addition, the cross-covariance

$$\mathrm{E}\{\hat{x}_e(t+1)\delta y(t)^*\} = (B_t + L_t D_t)D_t^* + (A_t + L_t C_t)X_t C_t^* = 0, \tag{3.17}$$

in light of the fact $L_t = -(B_t D_t^* + A_t X_t C_t^*)(D_t D_t^* + C_t X_t C_t^*)^{-1}$. We note that the error covariance in (3.15) have the same form as the original random process (3.12) except that (A_t, B_t) are replaced by $(A_t + L_t C_t, B_t + L_t D_t)$. Thus denoting $\tilde{\Phi}_{t,k}$ as the transition matrix from time k to $t-1$ associated with $(A_t + L_t C_t)$ and $\tilde{\Phi}_{t,k} = (A_{t-1} + L_{t-1}C_{t-1}) \cdots (A_k + L_k C_k)$. We obtain that for $t > k \geq 0$,

$$\begin{aligned} \mathrm{E}\{\delta y(t)\delta y(k)^*\} &= C_t \tilde{\Phi}_{t,k} X_k C_k^* + C_k \tilde{\Phi}_{t,k+1}(B_k + L_k D_k)D_k^* \\ &= C_t \tilde{\Phi}_{t,k+1}[(A_k + L_k C_k)X_k C_k^* + (B_k + L_k D_k)D_k^*] = 0, \end{aligned} \tag{3.18}$$

If $k = t$, then $\mathrm{E}\{\delta y(t)\delta y^*(k)\} = C_t X_t C_t' + D_t D_t'$ for $x_e(t)$ and $v(t)$ are independent with each other. □

3.3 Replay Attack

Since the networked control system (NCS) employs the information technology (IT) to implement the system control through a shared network, it is vulnerable to malicious attacks. A typical vicious attacker is the replay attack that attacks the NCS by concealing the monitors or feeding the false information to the controllers. The replay attack undermines the system stability and can damage the system infrastructures that typically employ many control systems. Therefore, detection of the replay attack is a very important subarea of the security in NCSs. In this section, the replay attack will be described.

An example of the known replay attack is launched by the Stuxnet malware, which allegedly is designed to attack the Iran's uranium enrichment plant in 2009 and caused one fifth of the centrifuges damaged [13]. According to the news media [4], Stuxnet secretly recorded the normal operations status when system runs under normal condition, and then

played those readings back to the system operators when the systems failed. It would appear to the operator that everything was running smoothly while the system was already damaged. It prevents the system from doing some actions to prevent abnormal operation. Since 2009, the Stuxnet malware has been spread all over the world, which has been detected on the computer systems in Iran, India, Indonesia and other countries [13]. This impels us to develop methods to protect our infrastructures from the replay attack.

The first paper discussed the replay attack in networked control system is [6] that was published in 2009. The idea of this paper is to inject a white Gauss signal in the control input, and test the estimation residue for the output estimation error of the Kalman filter. In [6], the χ^2 failure detector used to detect the presence of the replay attack based on the assumption that, the control system is discrete time linear invariant (LTI) with an infinite horizon Linear quadratic Gaussian (LQG) controller in which a Kalman filter is employed to estimate the system's state. The output estimation error variance of the Kalman filter will be larger if the replay attack exists, than that when the replay attack is absent. This is because the added Gauss signal is known to the controller and can be canceled in the Kalman filter when replay attack is absent; Otherwise, it cannot be canceled that results in higher output estimation error. Although the injected authentication signal helps to detect the replay attack, it degrades the system control performance. In order to reduce the degradation of the system control performance, a new detection strategy is proposed in [9]. By periodically injecting the Gauss white noise into the control input, we can tradeoff the detection rate versus system control performance. A new method is developed in [11] that employs the channel noise and measurement noise to detect the replay attack, which avoids the injection of the authentication noise, and hence avoids degrading the control performance. Besides above methods, the game theory is introduced in [10] to detect replay attack. It opens a new way to tradeoff the replay attack detection rate and system control performance. In [9], [14] the replay attack detection strategy that injecting the Gaussian noise in the control input method is discussed in smart grid.

CHAPTER 4
FREQUENCY HOPPING METHOD

The existing detection method for replay attack as proposed in [6] does not have good detection rate, because the injected authentication white signal cannot have large variance. If it has large variance, the control system performance will be degraded significantly. The reason lies in the white signal that is a wide-band signal, and it cannot have both small mean power and high detection rate. In order to improve the detection rate and reduce the adverse impact on control system performance, a new detection method is proposed in our study. The narrow-band signal rather than the white signal is injected in the control input. The narrow-band signal is centered at a certain frequency, and it can have small variance. Thus it dose not degrade the control system performance seriously. More importantly the proposed narrow-band signal helps to achieve much better detection rate than that of the white noise, if both have the same variance.

4.1 White Noise Method

Mo and Sinopoli [6] are the first to consider the replay attack in the NCS that employs the LQG controller. Their detection method for replay attack is based on the feedback control system shown in Figure 2.2 of Chapter 2. The main idea for detecting the replay attack in the LQG based NCS is to inject an authentication white signal in the control input and to test the estimation residue of the output estimation error of the Kalman filter used in the LQG controller. In the following we outline the detection method proposed in [6].

For the linear time invariant generalized plant model described in the previous chapter, assumptions on $D_{11} = D_{22} = 0$, $D_{12}^* C_1 = 0$, and $B_1 D_{21}^* = 0$ are assumed in [6] for the simplicity reason. Hence the state space description for the generalized plant model is given by

$$\begin{aligned} x(t+1) &= Ax(t) + B_1 d(t) + B_2 u(t), \\ w(t) &= C_1 x(t) + D_{12} u(t), \\ y(t) &= C_2 x(t) + D_{21} d(t), \end{aligned} \tag{4.1}$$

where $x(t) \in \mathbb{R}^n$ is the vector of state variables at time t, $d(t) \in \mathbb{R}^n$ is the process noise at time t, $d(t)$ and x_0 are the independent Gaussian random variables. As a result, the controller and estimator gains of the LQG controller can be obtained as

$$F = -(R + B_2^* X B_2)^{-1} B_2^* X A, \tag{4.2}$$

$$L = -AYC_2^*(\tilde{R} + C_2 Y C_2^*)^{-1}, \tag{4.3}$$

respectively, where $X \geq 0$ and $Y \geq 0$ are the stabilizing solutions to the following respective Algebraic Riccati equations (AREs):

$$X = A^* X A + C_1^* C_1 - A^* X B_2 (R + B_2^* X B_2)^{-1} B_2^* X A, \tag{4.4}$$

$$Y = AYA^* + B_1 B_1^* - AYC_2^*(\tilde{R} + C_2 Y C_2^*)^{-1} C_2 Y A^*. \tag{4.5}$$

Set the system control input as

$$u(t) = u_*(t) + u_\triangle(t), \tag{4.6}$$

where $u_*(t) = F\hat{x}(t|t-1)$ is the optimal LQG control input and $u_\triangle(t)$ is the injected authentication signal. See Figure 4.1 for the LQG based feedback control system. The output estimation error $\delta y(t) = y(t) - C_2\hat{x}(t|t-1)$ is temporally white in the absence of the replay attack. In this case the covariance of this error is given by

$$\Omega^2 = \mathrm{E}\{[y(t) - C_2\hat{x}(t|t-1)][y(t) - C_2\hat{x}(t|t-1)]'\} = \tilde{R} + C_2 Y C_2'. \tag{4.7}$$

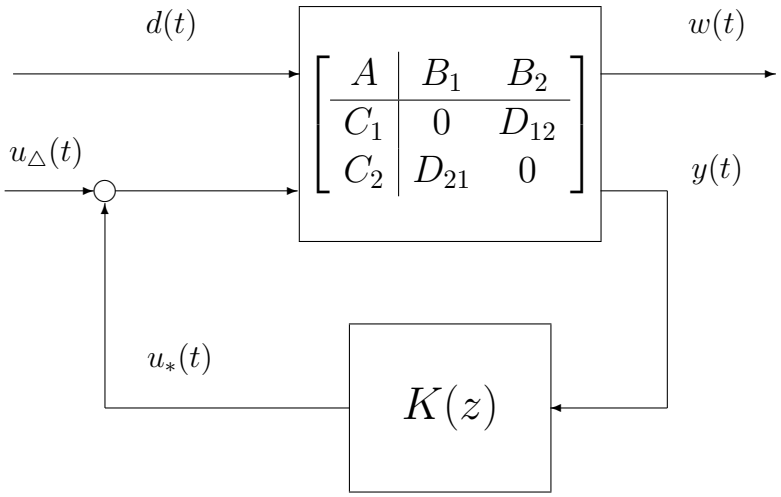

Figure 4.1: LQG control system with injected authentication signal

Let p be the dimension of $y(t)$. Defining $\varepsilon(t) = \Omega^{-1}[y(t) - C_2\hat{x}(t|t-1)]$, yields

$$\begin{aligned} \tfrac{1}{p}\mathrm{E}\{\varepsilon(t)'\varepsilon(t)\} &= \tfrac{1}{p}\mathrm{T_r}[\mathrm{E}\{\varepsilon(t)\varepsilon(t)'\}] \\ &= \tfrac{1}{p}\mathrm{T_r}\{\Omega^{-1}\mathrm{E}\{\delta y(t)\delta y(t)'\}\Omega^{-1}\} \\ &= \tfrac{1}{p}\mathrm{T_r}\{I_p\} = 1. \end{aligned} \tag{4.8}$$

It follows that $\varepsilon(t)$ is both temporally and spatially white. If the replay attack is present, then it is shown in [6] that $\frac{1}{p}\mathrm{E}\{\|\varepsilon(t)\|^2\}$ is greater than 1, but how much greater depends on the mean power of the injected white noise. The above analysis leads to the following χ^2 failure detector:

$$\frac{1}{Np}\left(\sum_{k=t-N}^{t}\|\varepsilon(k)\|^2\right) \gtrless \tau, \tag{4.9}$$

where τ is a threshold and N is the detection window size. In practice, it is desirable to have big detection rate and small false alarm rate. However, if $\tau \gg 1$, then both the detection rate and false alarm rate become small. On the other hand, if $\tau \ll 1$, then both the detection rate and false alarm rate become big. Hence there is a tradeoff between the detection rate and false alarm rate by designing an appropriate threshold τ.

Consider the LQG control for the temperature control system discussed in [6], that aims at controlling the temperature inside a room. Suppose that T^* is the desired temperature and $T(t)$ is the temperature of the room at time t. A simple plant model for the temperature control system can be described by

$$\begin{aligned} x(t+1) &= x(t) + u(t) + v_p(t), \\ y(t) &= x(t) + v_m(t) \end{aligned} \tag{4.10}$$

where the system state is $x(t) = T(t) - T^*$, $u(t)$ is the control input, $v_p(t)$ is the process noise, $y(t)$ is the measurement of the temperature tracking error, and $v_m(t)$ is the measurement noise.

It is assumed in [6] that the process noise $v_p(t)$ and measurement noise $v_m(t)$ are independent to each other, and they have the variance 1 and 0.1 respectively. Setting

$$w(t) = \begin{bmatrix} 1 \\ \\ 0 \end{bmatrix} x(t) + \begin{bmatrix} 0 \\ \\ \sqrt{0.1} \end{bmatrix} u(t) \tag{4.11}$$

as in (4.1) results in the state feedback and state estimation gains

$$F = -0.618, \qquad L = -0.916 \quad ,$$

respectively. If no authentication signal is injected, then the LQG cost is $J = 1.7096$. If an authentication white signal is injected at the control input with variance v_{ad}, then the LQG cost is changed to

$$J' = J + 2.618 v_{ad}. \tag{4.12}$$

Following the study in [6], we also carried out the simulation study for this particular example. In the following simulation, we set the simulation time length to be 200s, and replay attack takes place at $t = 100s$. The delay time τ can be set advance or randomly decide by the replay attacker. The system output $y(t)$ will be τ seconds delay after the replay attack takes place, giving rise to

$$y_a(t) = y(t - \tau), \qquad t \geq \tau. \tag{4.13}$$

In order to obtain the statistical detection rate, 2000 trials are carried out in every simulation. We also set the false alarm rate to be 5% at each trial.

Figure 4.2 shows the detection rate of χ^2 failure detector for replay attack when the detection window size is $N = 5$, the delay time $\tau = 100s$, and no authentication signal is injected in the system control input. From Figure 4.2, we find χ^2 failure detector successfully detects replay attack at the beginning of attack, but the detection rate goes to zero as time goes. The reason of χ^2 failure detector transiently detects replay attack can be developed as follows.

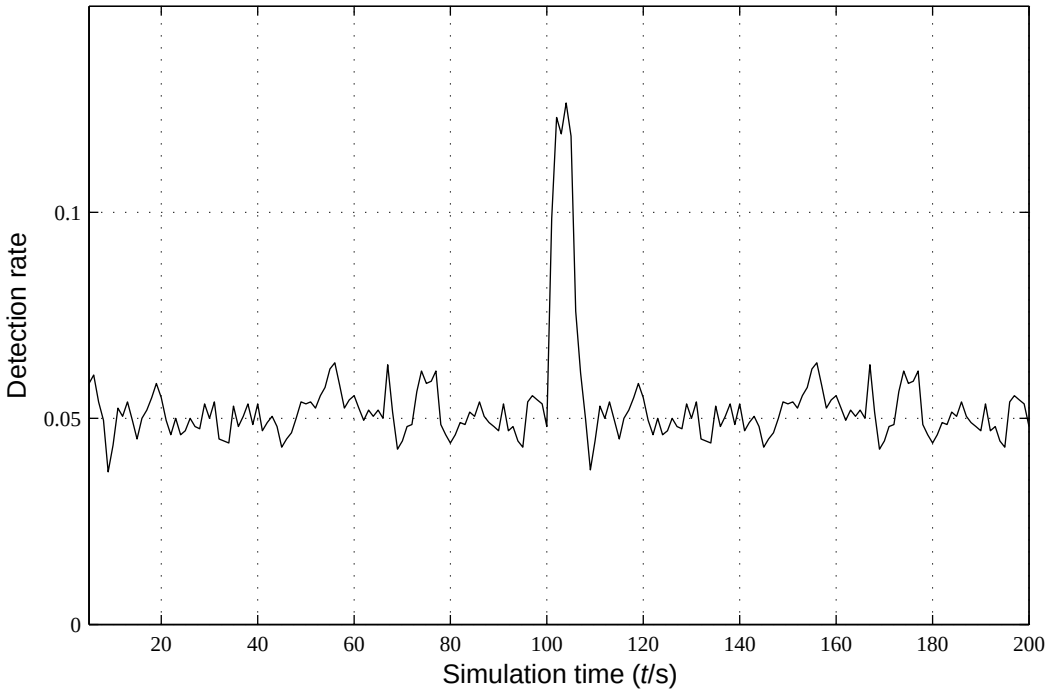

Figure 4.2: Detection rate without injecting authentication signal

According to (4.10) and (4.11), we obtain the estimate output error referring to (3.15) in proposition of Chapter3.

$$\begin{aligned}
\delta y(t+1) &= \tilde{y}(t+1) - \hat{y}(t+1) \\
&= \{C_2\tilde{x}(t+1) + D_{21}\tilde{v}_m(t+1)\} - \{C_2\hat{x}(t+1|t)\} \\
&= C_2\left\{A\tilde{x}(t) + B_1 v_p(t) + B_2 F\hat{\tilde{x}}(t|t)\right\} + D_{21}\tilde{v}_m(t+1) - C_2\{A\hat{x}(t|t) + B_2 F\hat{x}(t|t)\} \\
&= C_2 A\{\tilde{x}(t) - \hat{x}(t|t)\} + C_2 B_2 F\left\{\hat{\tilde{x}}(t|t) - \hat{x}(t|t)\right\} + C_2 B_1 v_p(t) + D_{21}\tilde{v}_m(t+1)
\end{aligned} \tag{4.14}$$

where $\tilde{y}(t+1)$ is the false feedback signal, and $\hat{\tilde{x}}(t|t) \neq \hat{x}(t|t)$ and $\tilde{x}(t) \neq x(t)$ since replay attacker feedbacks the previous system state to control system. We find that $\delta y(t+1)$ should be very small when there is not replay attack, because $\tilde{x}(t) - \hat{x}(t|t)$ is approximate to zero, $\hat{\tilde{x}}(t|t) - \hat{x}(t|t)$ is zero, and measurement noise and process noise do not provide large error. Otherwise, the output estimation error can be large unless the false feedback signal is carefully designed.

In Figure 4.3, we find that the χ^2 failure detector cannot detect replay attack at the beginning of the attack. Moreover, the delay time in Figure 4.3 $\tau = 6$ which is defined by replay attacker. This is because the 95th control system output is the optimal false signal that is close to the system output at $100s$, and it can minimize the output estimation error to avoid being detected by χ^2 failure detector. Because the χ^2 failure detector fails to detect the replay attack, Mo and Sinopoli proposed to inject white Gaussian authentication signal in control input to detect replay attack in [6]. The results in their paper are as follows.

Figure 4.4, Figure 4.5, and Figure 4.6 show the detection rate with different detection window size when the injected white Gaussian signal of variance 0.2, 0.4, and 0.6, respectively. The delay time τ is decided by the replay attacker.

These three figures indicate two features: 1) the bigger the detection window size, the higher the detection rate; 2) the larger variance of authentication signal yields higher detection rate. However, the large window size implies large time delay for the detection. The large variance of the injected authentication signal implies poor system control performance.

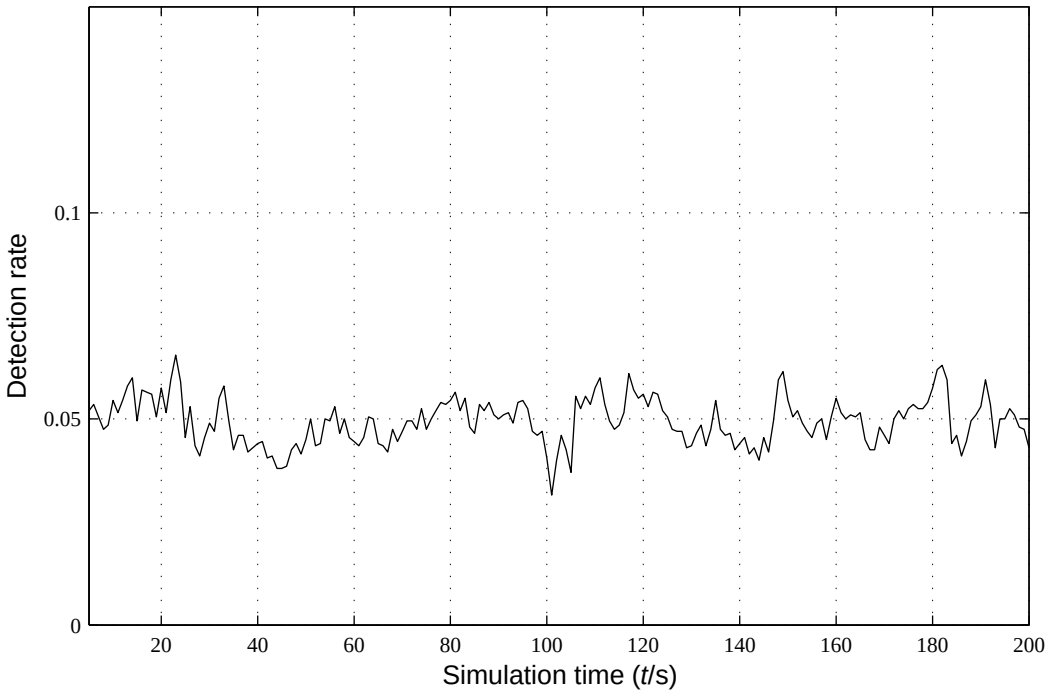

Figure 4.3: Detection rate under intelligent replay attack

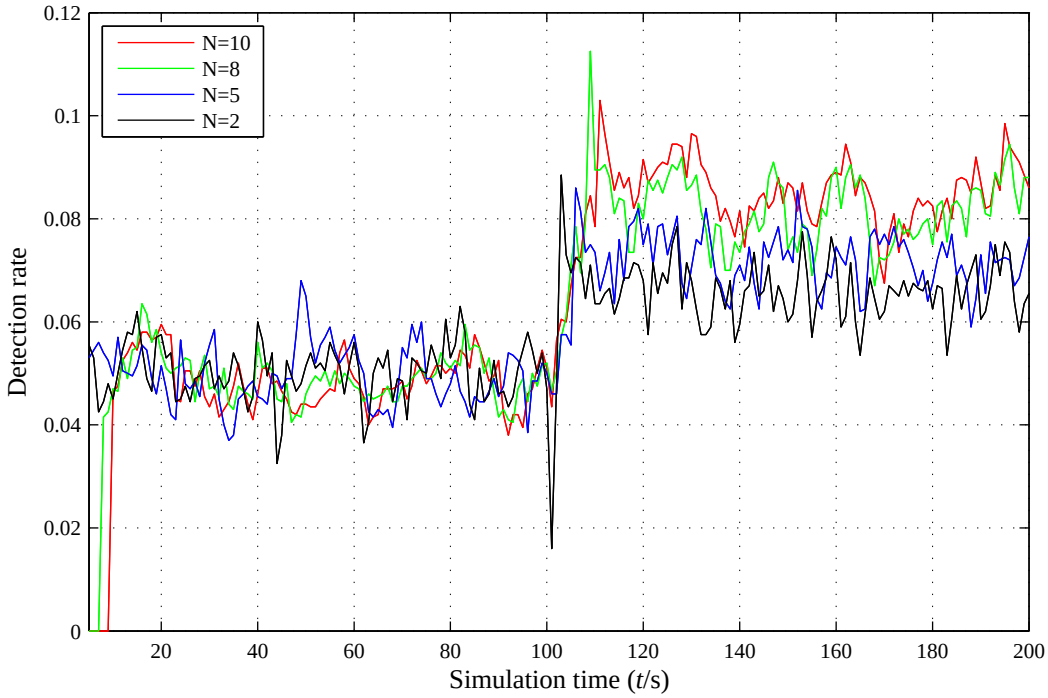

Figure 4.4: Detection rate with injected white Gaussian signal of variance 0.2

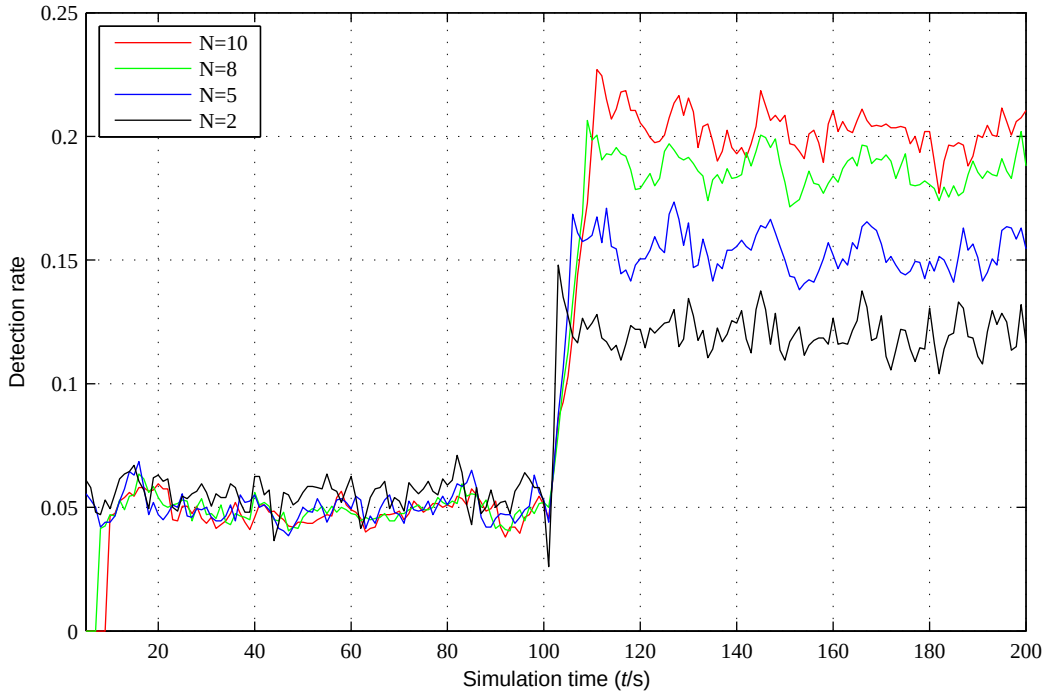

Figure 4.5: Detection rate with injected white Gaussian signal of covariance 0.4

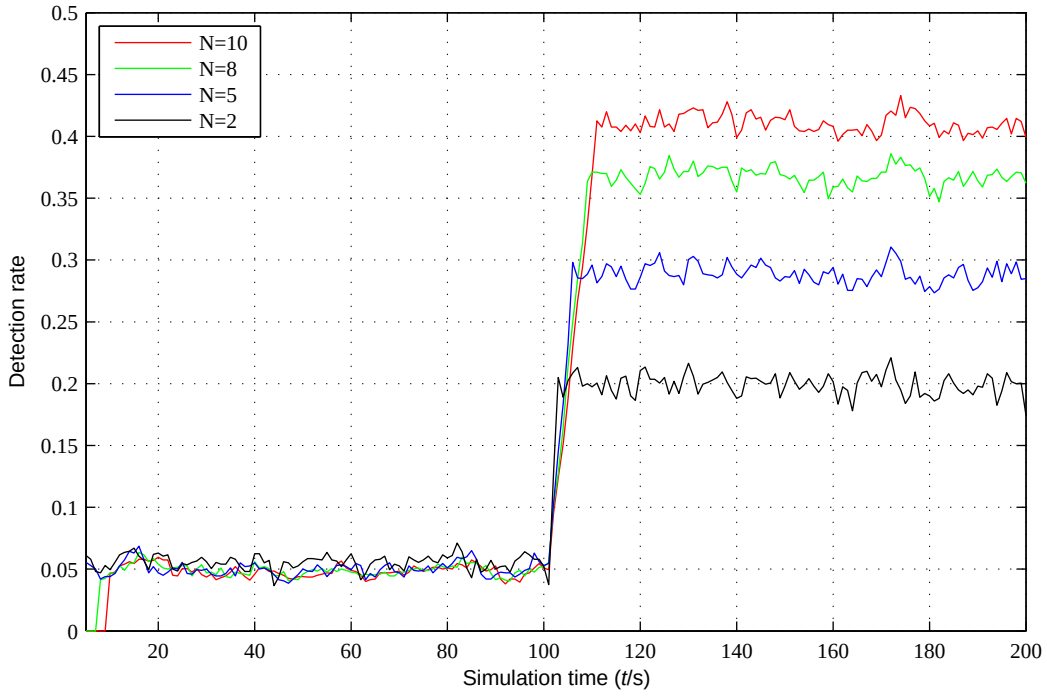

Figure 4.6: Detection rate with injected white Gaussian signal of covariance 0.6

With 0.2, 0.4, and 0.6 for the variance of the injected white authentication signal, the highest detection rate is 11.5%, 23%, and 44% respectively, which correspond to the loss of LQG performance is 30.6%, 61.25%, and 91.88%, respectively, compared with the optimal LQG cost. It is noticed that the highest detection rate is 44% when the variance of the injected authentication signal is 0.6 and detection window size is $N = 10$. This highest detection rate scarifies 91.88% of system control performance with time delay of $10s$ in detecting replay attack. Overall, the detection method for the replay attack with injected white Gaussian signal is not efficient and practical. Therefore, more efficient detection method should be worked out to tradeoff the detection rate and the system control performance.

Figure 4.7 shows the detection rate of injected white Gaussian authentication signal with different variance but the same detection window size $N = 5$. In the next section, we will

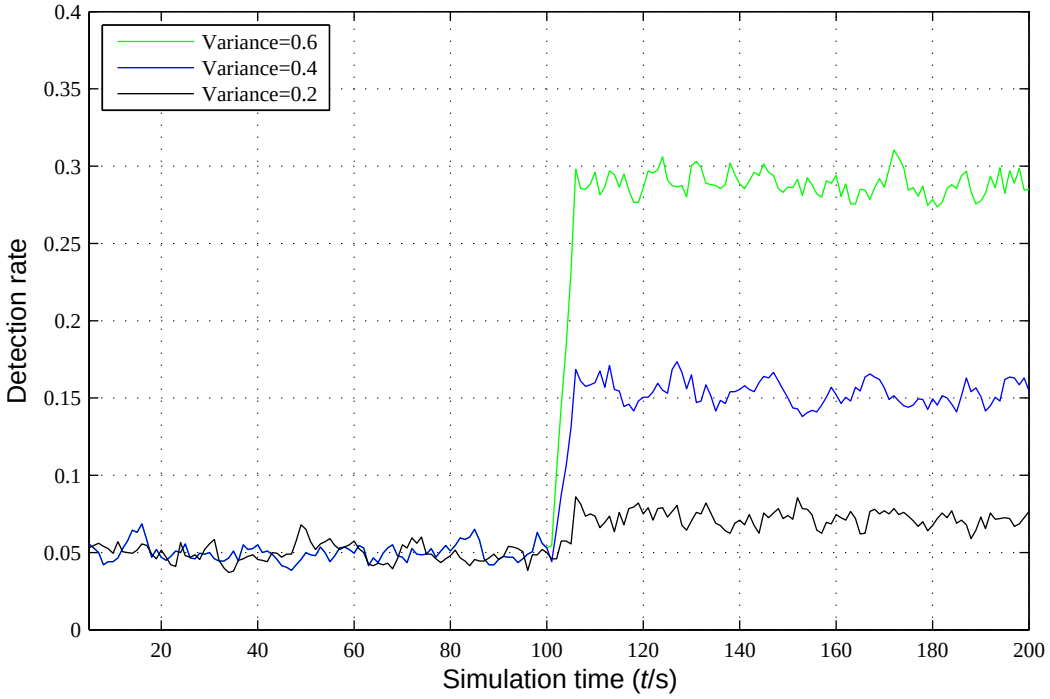

Figure 4.7: Detection rate with injected white Gaussian signal of detection window size 5

introduce a new detection method by injecting a narrow-band signal in the control input to improve the detection rate without sacrificing much the control system performance.

4.2 Spectrum Detection Method

It is desirable to develop detection methods that have high detection rate, while keeping the minimum impact on the control system performance. The existing method cannot achieve this goal, because it injects white authentication signal and the PSD spreads over all frequencies. In light of the fact that the mean power of the authentication signal cannot be large in order to minimize the adverse effect on the control performance, the way to overcome the weakness of the existing method in [6] is to replace the white authentication signal by narrow-band signals. We propose to inject the following narrow-band signal:

$$u_{\triangle}(t) = \alpha \cos(\omega_0 t + \theta) \tag{4.15}$$

over $[t_0, t_0 + T_w]$, where T_w specifies the time horizon, and α and θ are random variables, uniformly distributed over $[0, \alpha_{max}]$ and $[0, 2\pi)$, respectively.

Comparing to the white noise detection method, the spectrum detection method, provides higher detection rate, and is more sensitive to replay attack. This is because the injected narrow-band signal with the same variance does not affect the system control performance too much, but offers a higher detection rate than that of the white signal at frequency ω_0. In the absence of replay attack, the output estimation error $\delta y(t)$ has the same covariance as in (4.7). That is, the injected cosine signal is canceled completely. Recall that $u_{\triangle}(t)$ is known by the controller. However, when replay attack is present, then the injected cosine signal cannot be canceled completely, if the adversary has no knowledge on the frequency ω_0. As a result, the output estimation error $\delta y(t)$ will have a cosine component at frequency ω_0. Therefore, we can employ the spectrum estimation method to detect replay attack. In this section we will use spectrum detection method to detect replay attack. A non-parametric estimation method is summarized as follows [15]. We only consider the case $p = 1$.

For a given discrete time signal $\{s(k)\}_{k=1}^{N}$, the simplest method to estimate its PSD at frequency ω_h can be obtained according to [15] (page 22-24).

$$\hat{\Phi}_p(\omega_h) = \frac{1}{N}\left|\sum_{k=1}^{N} s(k)e^{-j\omega_h(k-1)}\right|^2. \tag{4.16}$$

The standard biased ACS estimate of $s(k)$ can be obtained as

$$\hat{R}_p(\tau) = \frac{1}{N}\sum_{k=\tau+1}^{N} s(k)s'(k-\tau), \quad 0 \leq \tau < N-1. \tag{4.17}$$

A different estimate of the PSD can be obtained as

$$\hat{\Phi}_c(\omega_h) = \sum_{\tau=-(N-1)}^{N-1} \hat{R}_c(\tau)e^{-j\omega_h\tau}. \tag{4.18}$$

where $\hat{R}_c$ is the standard unbiased ACS estimate and it holds

$$\hat{R}_c(\tau) = \frac{1}{N-\tau}\sum_{k=\tau+1}^{N} s(k)s'(k-\tau), \quad 0 \leq \tau < N-1. \tag{4.19}$$

The unbiased ACS estimate has a windowing effect and offers a more sophisticated estimation method which introduces the windowing technique by taking the PSD estimate at frequency ω_h as

$$\hat{\Phi}_s(\omega_h) = \sum_{\tau=-(N-1)}^{N-1} \text{win}(\tau)\hat{R}_s(\tau)e^{-j\omega_h\tau}. \tag{4.20}$$

The above cover the case of ACS estimate are in the average sense. The advantages and disadvantages of common used window as Barlett, Hanning, Hamming, and Blackman will not be discussed here.

By utilizing the spectrum estimation method, the simulation results of detecting replay attack are as follows.

Figure 4.8 shows the detection rate of replay attack with injected fixed amplitude and fixed frequency cosine authentication signal. In Figure 4.8, the amplitude, the frequency and the variance of the injected cosine signal are 0.6325, 1.26 and 0.2, respectively. The

detection window size is $N = 5$. The detection rate of the χ^2 failure detector and spectrum detection method are shown in Figure 4.8. The spectrum detection method provides higher detection rate than that of χ^2 failure detector. Moreover, the detection rate with injected fixed amplitude cosine signal is higher than that with injected white Gaussian signal under the same condition. Corresponding to the peak detection rate of 9% in Figure 4.7, the peak detection rate in Figure 4.8 is 14.2%. Although the detection rate is oscillating when injecting the cosine authentication signal in the system control input, it effectively detects the replay attack. However, there is a drawback to detect replay attack with injected sinusoidal authentication signal: The injected signal can be copied if the attacker is intelligent enough, causing this replay attack detection method to fail. According to our analysis, the spectrum detection method fails when the attacker knows the frequency ω_0 and sets the time delay to satisfy relation:

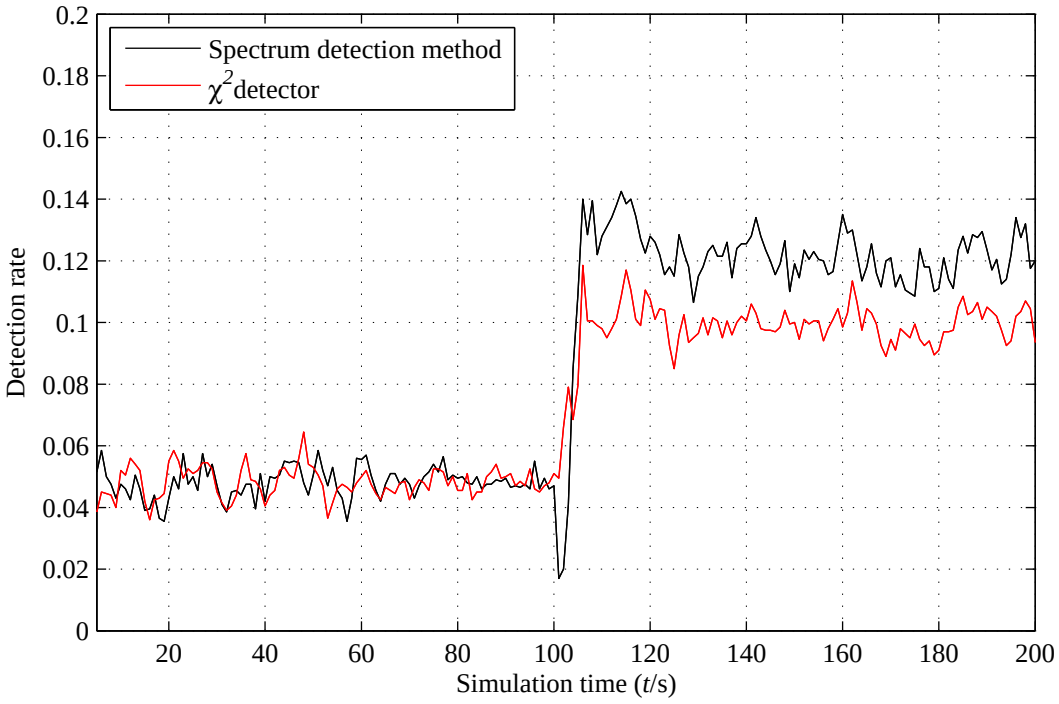

Figure 4.8: Detection rate with injected fixed amplitude cosine signal

$$\tau\omega_0 = 2\pi n. \tag{4.21}$$

By doing so, the injected cosine authentication signal is repeated in the attacking duration, and can thus be canceled in the Kalman filter.

Figure 4.9 shows that the spectrum detection method fails when the frequency of the injected authentication cosine signal is 1.2566 and the time delay $\tau = 100s$ that satisfies (4.21). The detection rate in Figure 4.9 validates the fact that the spectrum detection method can fail, if the adversary has the knowledge of the frequency of the injected sinusoidal signal. But it's interesting to notice that the detection rate of the χ^2 failure detector in Figure 4.9 is similar to that of Figure 4.2. Indeed, the pulse can also be canceled when the attacker feedbacks the optimal false signal satisfies the two conditions, one is the constraint of (4.21), and the other one is that the feedback false signal should as close as the system output at the attack moment.

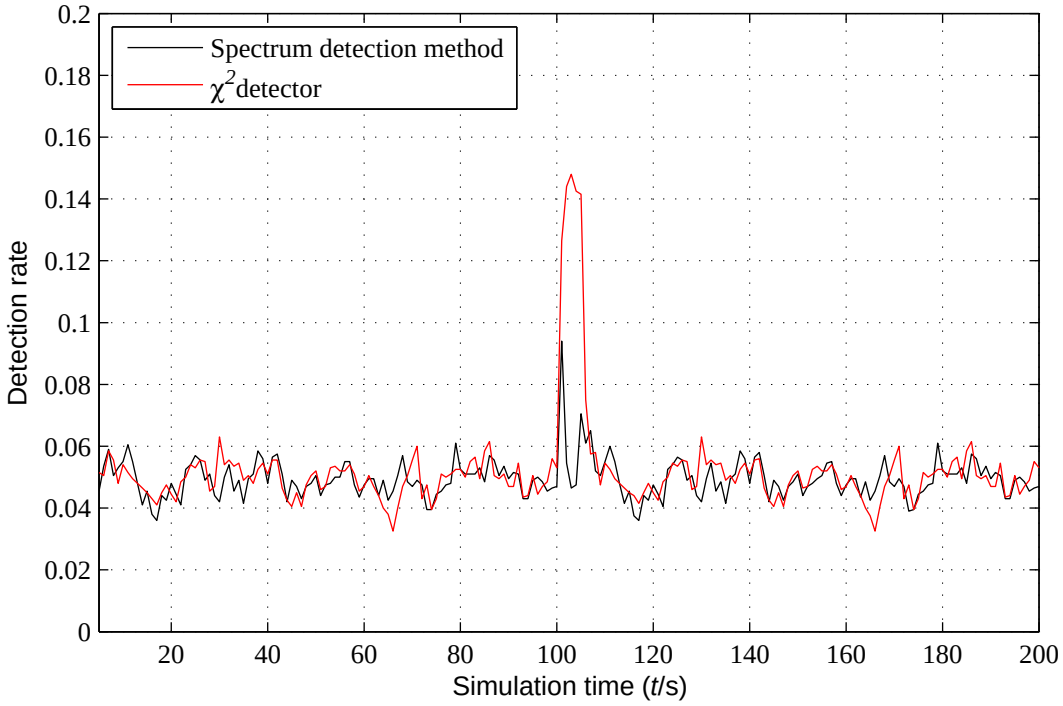

Figure 4.9: Detection rate with injected fixed amplitude cosine signal under the intelligent attack

Figure 4.10 is the simulation result when injecting random amplitude cosine signal with frequency 1.2566 in the control input and the time delay $\tau = 100s$. The detection rate is

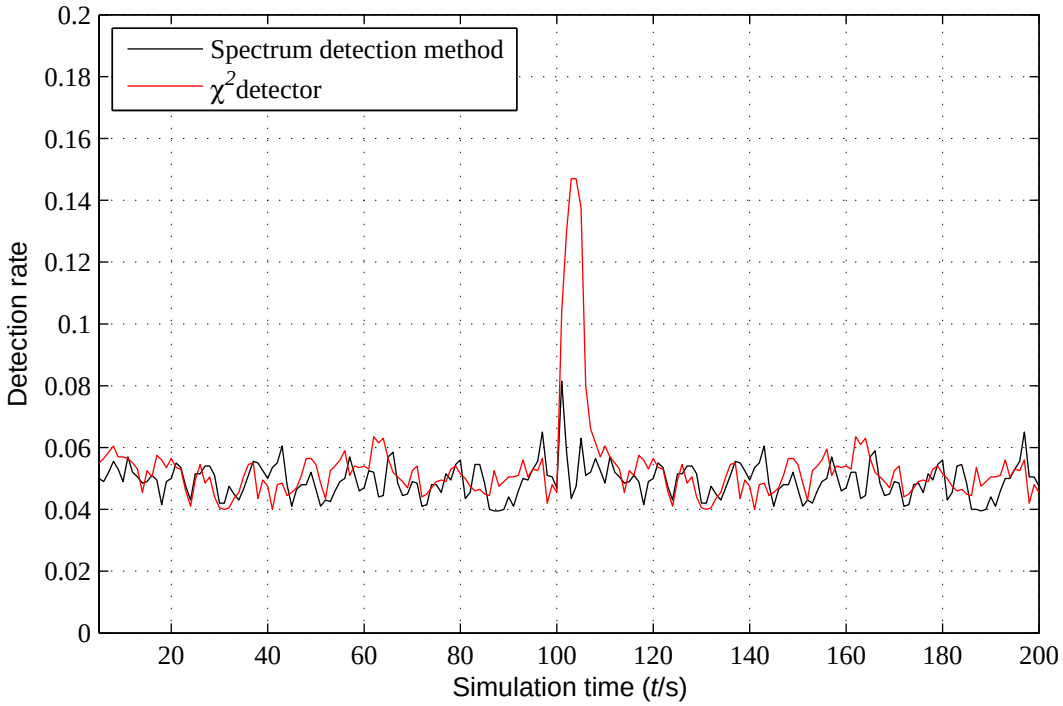

Figure 4.10: Detection rate with injected random amplitude cosine signal

similar to that in Figure 4.9. Indeed, it does not change too much even if we inject fixed frequency cosine authentication signal with randomly varying amplitude in the control input. The simulation results in in Figure 4.9 and Figure 4.10 illustrate the difficulty of using the spectrum method for detecting the replay attack.In order to prevent the adversaries from knowing the characteristics of the injected signal, we propose the other detection method in this thesis by injecting authentication signal with random amplitude and random frequency. Referring to (4.15), we set ω_0 to change from one time horizon to another time horizon. Hence we call it the frequency hopping method.

4.3 Frequency Hopping Method

Frequency hopping method that is referred to frequency hopping communication in which the frequency of the carrier signal varies from time to time to avoid interception and interruption, is introduced in this subsection to detect replay attack. Before developing the frequency hopping method, the frequency hopping communication is briefly discussed in the following subsection.

4.3.1 Frequency Hopping Communication

Frequency hopping has been widely used in military communication and Bluetooth transmission, since it has two outstanding properties: high security to protect from interception and good resistance to the narrow-band interference. The principle of frequency hopping communication is to extend the narrow-band signal from narrow-band to wide-band by multiplying the narrow-band signal with a wide-band signal. The covariance of the extended signal is very small at all frequencies in [16]. More importantly, the narrow-band signal shifts between different frequencies according to a encrypted pseudorandom sequence. Thus, it is difficult to be intercepted and has a strong resistance to the narrow-band noise. The frequency hopping method used in the thesis refers to frequency hopping spread spectrum (FHSS) communication technology, which will be briefly discussed next.

Consider using binary frequency shift keying (BFSK) as the first data modulation scheme to modulate the signal $s(t_c)$, which has been discussed in Chapter 2. The output signal of the first modulation can be obtained as [17]

$$s_d(t_c) = s(t_c)\cos\left(2\pi(f_0 + b_i f_\triangle)t_c\right), \qquad (i-1)T_s < t_c < iT_s, \tag{4.22}$$

where f_0 is the base frequency with unit Hertz, $f_\triangle$ is the frequency separator in the BFSK scheme, b_i is the ith bit of pseudo-noise sequence which is generated by linear feedback shift register (LFSR), LFSR will not be discussed here, T_s is the duration of a single bit, and t_c

is the continuous time variable. Suppose that the frequency f_i of the second modulation is also determined by the pseudo-noise sequence. Then the resulting signal is

$$\begin{aligned} s_p(t_c) &= s(t_c)\cos(2\pi(f_0 + b_i f_\triangle)t_c)\cos(2\pi f_i t_c) \\ &= s(t_c)(\cos(2\pi(f_0 + b_i f_\triangle + f_i)t_c) + \cos(2\pi(f_0 + b_i f_\triangle - f_i)t_c)). \end{aligned} \tag{4.23}$$

Eliminating the second part of the above sum, we can obtain the signal with frequency centered around $f_0 + f_i$. By doing reverse process, the original signal can be recovered when the pseudo-noise sequence and binary sequence are known by the receiver. When M-ary frequency shift keying (MFSK) scheme is applied in the modulation, b_i in (4.22) becomes a variable that changes between $[0, 1, \cdots M]$. A MFSK example can be found in Figure 4.11, T is the duration of a bit, T_s is the duration of signal element, T_c is the interval duration of frequency hopping in sub-channels.

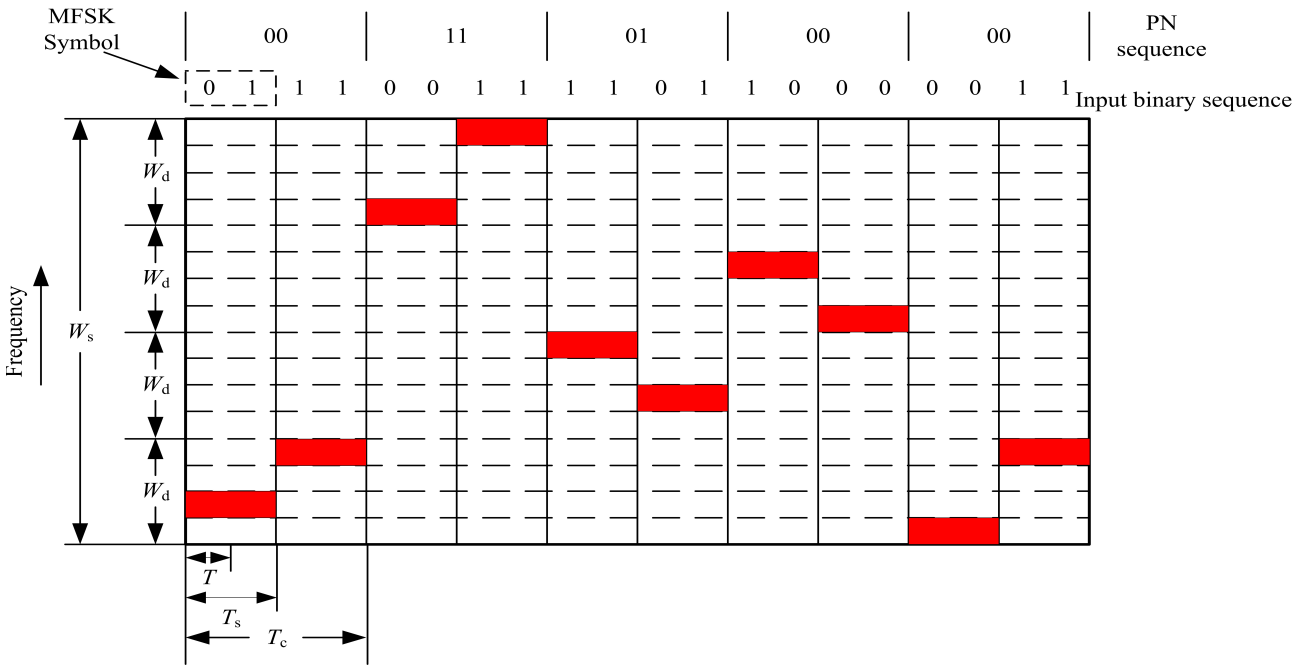

Figure 4.11: Slow Frequency Hop Spread Spectrum Using MFSK (M=4, k=2)

4.3.2 Proposed Detection Method

To overcome the shortcoming of spectrum detection method proposed in Section 4.2, we employ frequency hopping technology in detecting replay attack. By randomly shifting the frequency of injected signal, we can encrypt the injected authentication signal to make it difficult to be copied. The simulation results are based on the temperature control system model discussed in Section 4.1 [6]. The difference from the previous two detection methods is to inject cosine authentication signal with random frequency in the control input. The frequency of cosine signal is controlled by a pseudo-noise sequence generator that randomly generates 5 different frequencies. They are 1, 1.2, 1.4, 1.6, and 1.8. We set the injected cosine authentication signal with different variance of 0.2, 0.4, and 0.6, respectively. The corresponding amplitude of injected signal are 0.6325, 0.8944, and 1.0954, respectively. We set the detection window size $N = 5$ and time horizon $T_w = 10$. The frequency of the injected cosine authentication signal will hop every $T_w = 10s$. We carry out simulation studies with injected cosine signal with fixed amplitude and random amplitude. The simulation results are as follows.

Figure 4.12 shows the detection rate of frequency hopping method with injected fixed amplitude cosine signal. The peak detection rate in Figure 4.12 is 35 %, when the variance of injected cosine authentication signal is 0.6 and the detection window size is $N = 5$. When the variance of the injected signal is 0.2, the detection rate of spectrum estimation method is not good enough. Moreover, the detection rate oscillates irregularly. But the detection rate of frequency hopping detection method is generally better than that of white noise detection method shown in Figure 4.7.

Figure 4.13 shows the detection rate of χ^2 failure detector when injecting the fixed amplitude cosine authentication signal in control input. The detection rate shown in Figure 4.13 does not change a lot from that of Figure 4.12.

Figure 4.14 shows the detection rate of frequency hopping method with the injected cosine signal of random amplitude. The amplitude of the injected signal are random variables

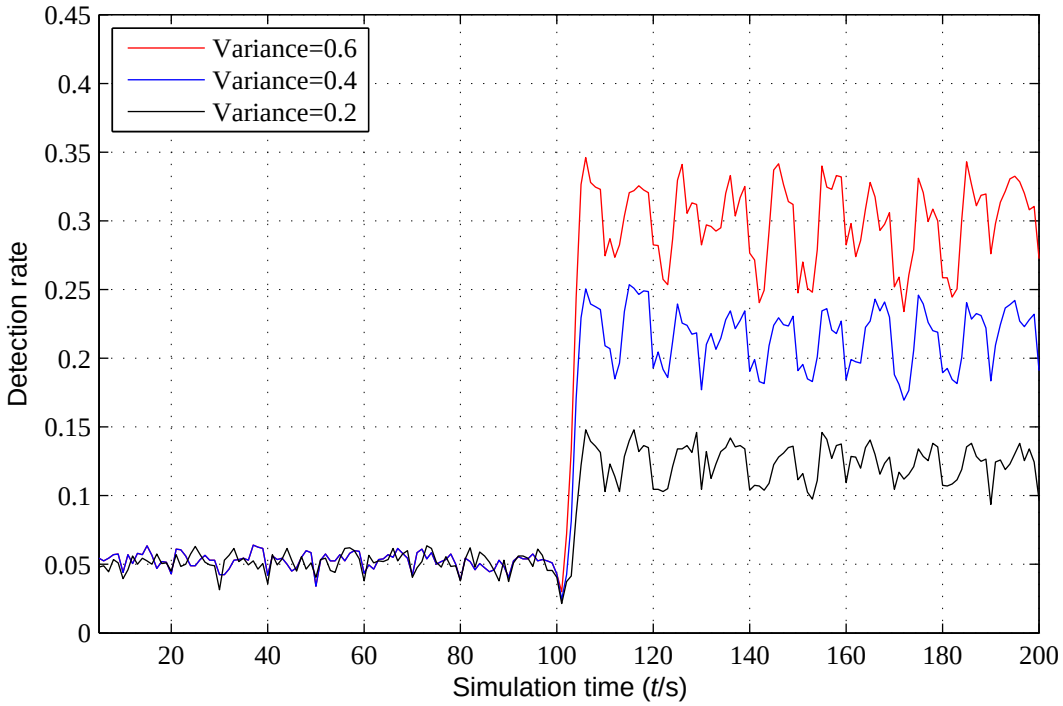

Figure 4.12: Detection rate with injected fixed amplitude cosine signal

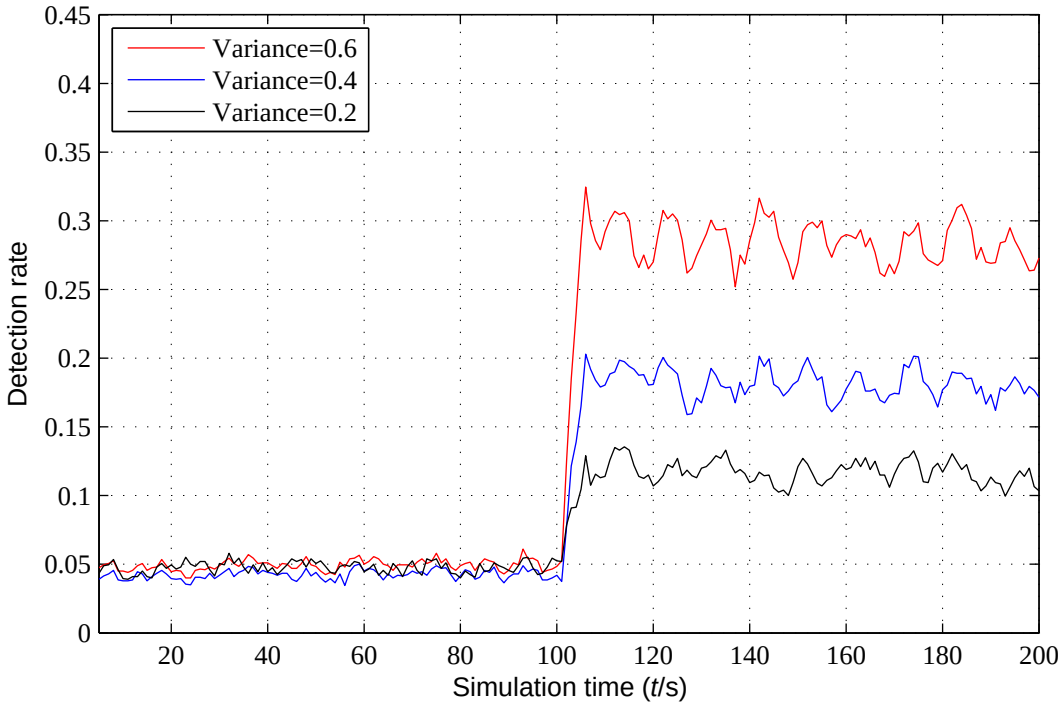

Figure 4.13: Detection rate of χ^2 failure detector with injected fixed amplitude cosine signal

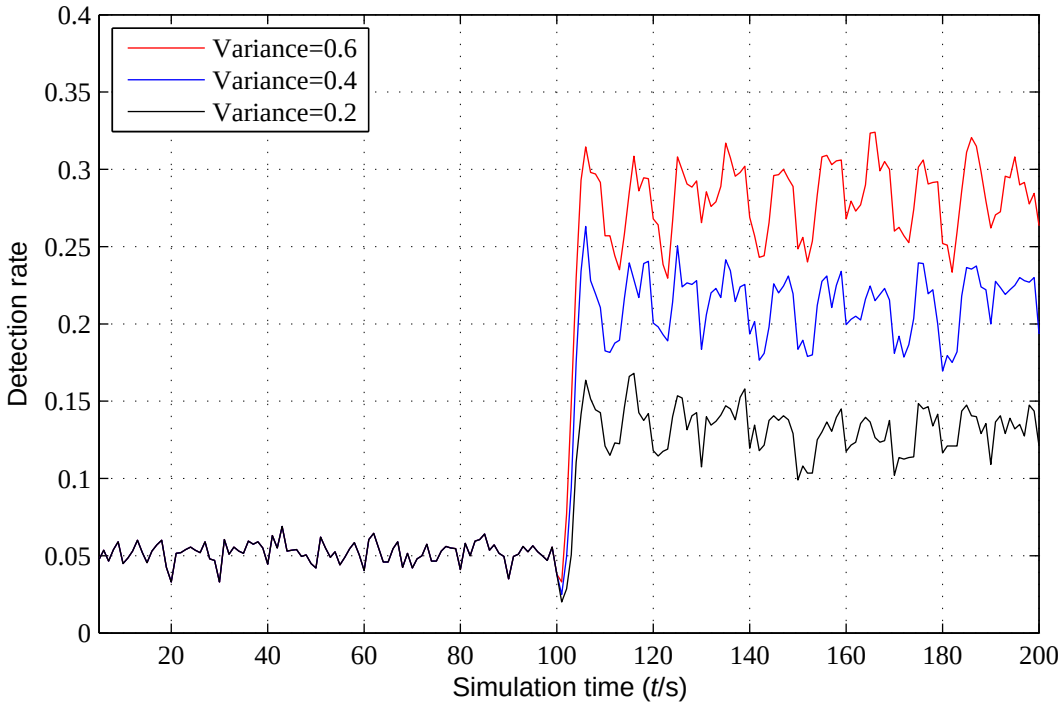

Figure 4.14: Detection rate with injected random amplitude cosine signal

between (0, 1.0954], (0, 1.5492], and (0, 1.8974], respectively. There is not a big difference between Figure 4.14 and Figure 4.12.

Figure 4.15 shows the detection rate of χ^2 failure detector when injecting random amplitude cosine authentication signal. Figure 4.12, Figure 4.13, Figure 4.14, and Figure 4.15 show that the frequency hopping method doesn't not improve the detection rate a lot than that of the χ^2 failure detector. Moreover, the detection rate of using frequency hopping method doesn't show a big progress than that of white noise method in the results. After carefully analysis the detection window size and (4.16), we find that we cannot obtain the accurate PSD when the detection window size is too small.

Therefore, we adjust the simulation conditions to do some simulation studies of frequency hopping method. We set the simulation time $T = 500s$, the replay attack takes place at 250s, the detection window size $N = 20$, and the time horizon $T_w = 60$. The time delay τ is decided by the intelligent replay attacker according to (4.21). The variance of the injected

authentication signal is 0.2 and 0.4, respectively. We do 2000 trials each time to obtain the statistic detection rate.

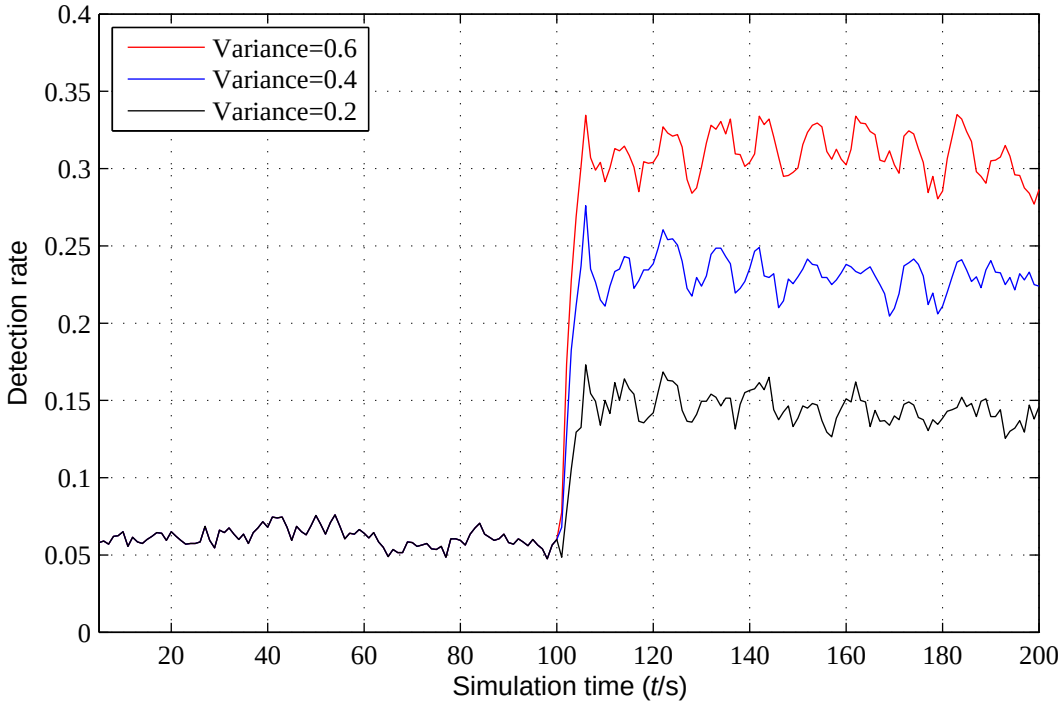

Figure 4.15: Detection rate of χ^2 failure detector with injected random amplitude cosine signal

Figure 4.16 shows the detection rate of the white noise method and frequency hopping method that with injected signal variance of 0.2 and 0.4, respectively. In Figure 4.16, $\mathrm{W}-\mathrm{variance}=0.2$ represents the detection rate of white noise method with the injected signal of variance 0.2. Slimily, $\mathrm{F}-\mathrm{variance}=0.2$ denotes the detection rate of frequency hopping method with the injected signal of variance 0.2. $\mathrm{W}-\mathrm{variance}=0.4$ and $\mathrm{F}-\mathrm{variance}=0.4$ have the similar meaning. The detection rate of the frequency hopping method periodically oscillates and drops between the time horizons. The shifting frequency induces the estimation error in calculating the PSD of output error.

Figure 4.17 shows the detection rate of the spectrum detection method and χ^2 failure detector with frequency hopping technology, respectively. The S.D.M with variance 0.2 means the detection rate of the spectrum detection method with injected signal of variance

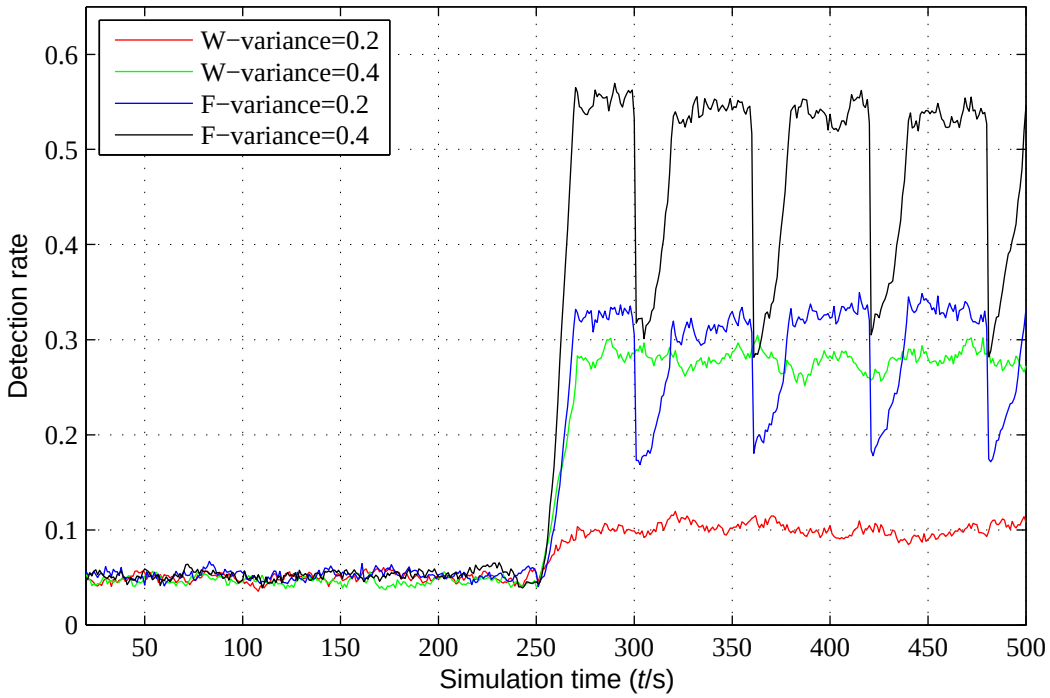

Figure 4.16: The detection rate comparison between white noise detection method and frequency hopping method

0.2. The similar meaning of S.D.M with variance 0.4. χ^2 with variance 0.2 and χ^2 with variance 0.2 means the detection rate of the χ^2 failure detector with injected signal of variance 0.2 and 0.4, respectively. The Figure 4.17 shows that the detection rate of χ^2 failure detector is smoother than that of the spectrum detection method, but the average detection rate is lower.

After adjusting the detection window size, we increase the detection rate of both the white noise detection method and the frequency hopping method. But Figure 4.16 shows that the detection rate of the frequency hopping detection method is higher than that of white noise method. It indicates that the frequency hopping method is better than white noise method. More importantly, the frequency hopping method improve the security of control system because this detection method can encrypt the injected signal. The encrypted control system strength the resistance of malicious intelligent attack. Therefore, we can claim that the frequency hopping detection method is more advanced than white noise method.

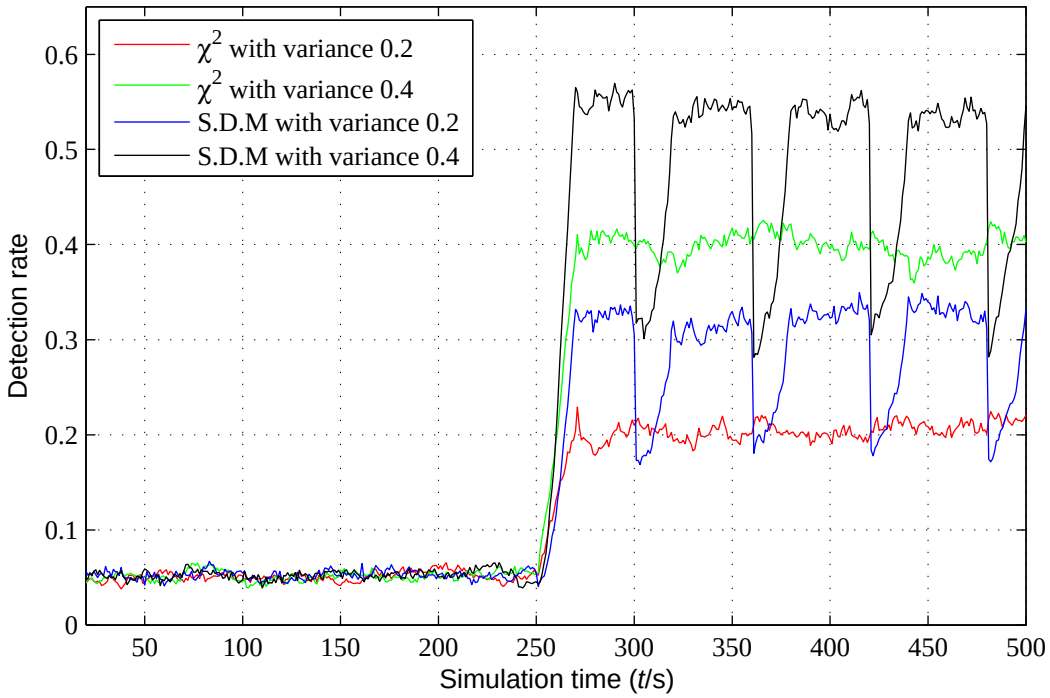

Figure 4.17: The detection rate comparison between χ^2 failure detector and spectrum detection method

Moreover, the simulation studies show that the spectrum detection method reveals better detection rate than χ^2 failure detector with the frequency hopping technology. Although the detection rate can be improved by increasing detection window size, both the frequency hopping method and the white noise method scarify the detection time. Both of these detection methods cannot perfectly tradeoff the control system performance, variance of the injected signal, and detection time. The more effective detection method of replay attack need to be studied in the future.

CHAPTER 5
CONCLUSION

With the advancement of automation and wide deployment of the information technology (IT), networked control systems (NCS) become more and more important in today's digital economy. Compared to the traditional control system, the NCS can reduce the cost, and is easy to maintain. More importantly, the NCS makes remote control possible, and enable robots and other controlled systems to work in hazardous environments where wired connection is not allowed or prohibited. As such the NCS is expected to be an essential part and plays a crucial role in future industry, agriculture, and military, because the underlying infrastructures are full of feedback control systems. However, along with the development and the application of the NCS, its security becomes a more and more critical issue. Due to the utilization of the IT, especially the shared wireless communication networks, NCSs are vulnerable to malicious attackers. In this thesis, we have focused on one type of attacks, referred to as *replay attack* that can be launched by malicious attackers from Cyber. Replay attacks can penetrate in control system secretely, reprogram embedded actuators and sensors, or copy the system information and feedback the false output data to the control system. Such attacks can destabilize control systems without being detected, or even destroy hardware facilities. More seriously, replay attacks can damage important military facilities of the country and cause huge financial loss. Therefore, it is crucial to develop efficient methods to detect replay attacks. Although there are some studies in the existing literature, the known solutions are not satisfactory which motivate this thesis research. We proposed a new method in this thesis to detect the replay attack and this new detection method is examined by our simulation studies. The thesis work is summarized in the following section.

5.1 Summary

In this thesis, we aimed at solving the detection problem for the replay attack. Since the traditional χ^2 detector does not perform well in detecting the replay attack by injecting

white authentication signal, a new effective detection method is proposed in this thesis. Our research on the replay attack detection problem are summarized next.

The existing method [6] injects white Gaussian noise as the authentication signal into the control input. Although it is capable of detecting replay attacks, the variance of the injected noises needs to be large, which degrades the control system performance. On the other hand large variance authentication signal degrades the control system performance. For this reason tradeoff has to be made between the detection rate and loss of the control system performance. There exists some works trying to tradeoff the detection rate and system control performance, but none of them achieves this goal. Basically the high detection rate cannot be obtained without injecting white Gaussian authentication signal with large variance, posing a significant challenge to the detection problem for replay attacks.

In this thesis, a new narrow-band authentication signal rather than the white Gaussian signal, is proposed to be injected to the feedback control system at the plant input. Compared to the white noise method that consists of the χ^2 detector and the white Gaussian noises, the spectrum detection method with injected narrow-band signal works better in detecting replay attacks. Specifically the PSD of the narrow-band signal concentrates at a fixed frequency and its neighborhood, contrasting to the PSD of the injected white Gaussian signal, which spans uniformly to the whole spectrum. In addition it is possible to obtain high detection rate by injecting narrow-band authentication signal with large variance without adversely affecting control system performance seriously. Indeed we can inject the narrow-band authentication signal at the frequency that is far away from the frequency content of the control signal.

The high detection rate based on the spectrum detection method can be obtained by injecting the narrow-band authentication signal with fixed frequency and fixed amplitude in the control input. The detection rate curve of the spectrum detection method with narrow-band authentication signal can be seen in Figure 4.8. However, this high detection rate is obtained assuming that the product of the time delay and the frequency of the injected signal is not multiple of 2π. When the adversaries are intelligent enough, they can estimate the

frequency and the amplitude of the injected authentication signal, and set the time delay to be multiple of 2π. As a result, the spectrum detection method can fail in detecting the replay attack when the intelligent attack deploys the above strategy. This is validated by our simulation result in Figure 4.9 and Figure 4.10.

In order to protect the information of the injected authentication signal from being estimated by replay attackers, we propose to encrypt the frequency of the injected signal by employing the frequency hopping communication technology, which is termed as *frequency hopping detection method*. See Section 4.3 for details. When injecting the narrow-band authentication signal at high frequencies, better detection rates than that of the white noise method can be obtained, assuming the same variance for the narrow-band authentication signal and for the white Gauss authentication signal. Moreover the longer the detection window size is employed, can the better detection rate be obtained. Figure 4.16 demonstrates the effectiveness of the frequency hopping detection method. To be specific, it injects narrow-band authentication signal with smaller variance than that of the white Gauss authentication signal. Yet the simulation results show that that the frequency hopping detection method can provide better detection rate than that of the χ^2 detector associated with white Gauss authentication signal. However large detection window size implies large time delay that is the cost associated with our proposed frequency hopping detection method.

5.2 Future Studies

In this thesis, we have studied the detection of replay attacks. The frequency hopping detection method is proposed and shown to be successful in detecting replay attacks. However, the research work in this thesis is not completed yet. The following outlines possible directions for future studies in this important research problem area.

1. In [6], Mo and Sinopoli provide the integral theoretic analysis of the relationship between the detection rate of the replay attack, and the LQG performance loss when injected authentication signals are white Gaussian noises. These analysis results help

readers to understand the quantitative tradeoffs between the detection rate and performance loss using the χ^2 detector. Similar to [6], the theoretical study on the use of narrow-band signal in detection of the replay attack needs to be carried out. For instance the quantitative analysis on the loss of the LQG performance cost needs to be derived. At present we do not have an explicit expression on the LQG cost loss when the narrow-band signals are employed authentication signals.

2. Most of the existing works analyze the detection rate of the replay attack has been focused on the plant input by injecting the authentication signal at the control input. Because replay attacks employ delayed output measurements, injecting the authentication signal at the plant outputs should be more effective. In [11], it shows that the channel noise at the system output can be more effective than injected noises at the system input in detection of the replay attacks. It will be interesting to study how the authentication signal can be injected at the system output in order to improve the detection rate while keeping minimum adverse effects on the control system performance.

3. Even though the existing works and our work in this thesis demonstrate the effectiveness of the various detection methods, not all the control systems are based on LQG controller. Therefore, it is essential to study the detection method for replay attacks for more general types of the feedback control systems, including those based on Bode design methods, PID control, and $\mathcal{H}_\infty$ control.

REFERENCES

[1] P. Ogren, E. Fiorelli, and N. E. Leonard. "Cooperative control of mobile sensor networks: Adaptive gradient climbing in a distributed environment". *IEEE Trans. Automat. Contr.*, vol. 49:1292–1302, 2004.

[2] R. Olfati-Saber and R. Murray. "Consensus problems in networks of agents with switching topology and time-delays". *IEEE Trans. Automat. Contr.*, vol. 49(9):1520–1533, 2004.

[3] P. Seiler and R. Sengupta. "Analysis of communication losses in vehicle control problems". *American Control Conference, 2001. Proceedings of the 2001,* Arlington, USA, pages 1491–1496, Jun. 25-27, 2001.

[4] W.J. Broad, J. Markoff, and D.E. Sanger. "Israeli test on worm called crucial in iran nuclear delay". *The New York Times*, Jan. 15, 2011.

[5] David Kushner. "The real story of stuxnet". *IEEE Spectrum*, vol. 50:48–53, Mar. 7, 2013.

[6] Y. Mo and B. Sinopoli. "Secure control against replay attacks". in *Communication,Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on,* Monticello, USA, pages 911–918, Sept.30-Oct.2, 2009.

[7] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, A. Perrig H. Lee, and B. Sinopoli. "Cyber physical security of a smart grid infrastructure". *Proceedings of the IEEE*, vol. 100(1):195–209, Jan., 2012.

[8] Y. Mo, R. Chabukswar, and B. Sinopoli. "Detecting Integrity Attacks on SCADA Systems". *IEEE Transactions on Control Systems Technology*, vol. 22(4):1396–1407, July, 2014.

[9] T.-T. Tran, O.-S. Shin, and J.-H. Lee. "Detection of replay attacks in smart grid systems". in *Computing, Management and Telecommunications (ComManTel), 2013 International Conference on,* Ho Chi Minh City, Vietnam, pages 298–302, Jan. 21-24, 2013.

[10] F. Miao, M. Pajic, and G. J. Pappas. "Stochastic Game Approach for Replay Attack Detection". *Decision and Control (CDC), 2013 IEEE 52nd Annual Conference on,* Firenze, Italy, pages 1854–1859, Dec. 10-13, 2013.

[11] Bixiang Tang, Luis Alvergue, and Guoxiang Gu. "Secure networked control against replay attacks without injecting authentication noise". *Proceedings of 2015 American Control Conference,* Chicago, USA, pages 6028–6033, Jul. 1-3, 2015.

[12] Guoxiang Gu. *Discrete-Time linear System: Theory and Design with Application*, volume 1. Springer, 2012.

[13] Porche Isaac. "Stuxnet is the world's problem". *Bulletin of the Atomic Scientists*, Dec. 9, 2010.

[14] Kebina Manandhar, Xiaojun Cao, and Fei Hu. "Combating False Data Injection Attacks in Smart Grid Using Kalman filter". *Computing, Networking and Communications (ICNC), 2014 International Conference on,* Honolulu, USA, pages 16–20, Feb. 3-6, 2014.

[15] P. Stoica and R. L. Moses. *Spectral analysis of signals*, volume 1. Prentice Hall Upper Saddle River, NJ, 2005.

[16] R. C. T. Lee, Mao-Ching Chiu, and Jung-Shan Lin. *Communications Engineering-Essentials for Computer Scientists and Electrical Engineers*, volume 1. Singapore: John Wiley, and Sons, cop., 2007.

[17] Torrieri Don. *Principles of Spread-Spectrum Communication Systems*, volume 1. Springer, 2011.

VITA

Guofu Tang was born in the Guilin of Guangxi Province in China. He is the son of Zhihang Tang and Huagui Li. He received the bachelor degree of electrical engineering from Taiyuan University of Technology in 2009. He became a graduate student in Beijing Jiaotong University in 2010 and got the master degree of electrical engineering in 2013. In 2017, he received M.S. degree in Electrical Engineering from Louisiana State University.