The Islamic University of Gaza

Deanery of Graduate Studies

Faculty of Engineering

Computer Engineering Department

الجامعة الإسلامية- غزة

عمادة الدراسات العليا

كلية الهندسة

قسم هندسة الحاسوب

Securing Weight-Based AODV (WBAODV) Routing Protocol in MANETs:

Towards Efficient and Secure Routing Protocol

Submitted by:

Wisam Tawfiq Elmasry

Supervisor:

Dr. Aiman Abu Samra

"A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master in Computer Engineering"

Gaza, June

1431- 2010

Abstract

An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. There are number of routing protocols developed by researchers. Due to the nature of ad hoc networks, secure routing is an important area of research in developing secured routing protocols. Although researchers have proposed several secure routing protocols, their resistance towards various types of security attacks and efficiency are primary points of concern in implementing these protocols. After the evaluation of these protocols the results refer that they do not give complete protection against possible attacks and have some disadvantages on their performance.

In this research, we examined a new routing protocol called Weight-Based Ad hoc On-demand Distance Vector (WBAODV) routing protocol which is efficient and superior of the standard Ad hoc On-demand Distance Vector (AODV) routing protocol in performance, but is not secure. So we proposed a new secure routing protocol based on WBAODV which will be efficient and also immune against the most commonly possible routing attacks. Finally we analyzed the proposed protocol against many attacks to ensure its security and also subject it to extensive simulation tests using JiST/SWAN simulation tool with the most commonly well-known ad hoc performance metrics to ensure its efficiency.

Keywords: Weight-based routing strategy, Routing attacks, Secure routing protocol, Mobile Ad hoc Networks.

عنوان البحث:

تأمين برتوكول التوجيه المعتمد على الأوزان في الشبكات اللاسلكية العشوائية : نحو بروتوكول توجيه جديد آمن و فعال

ملخص البحث:

الشبكة اللاسلكية العشوائية هي عبارة عن مجموعة من الأجهزة اللاسلكية المتنقلة و التي تشكل تلقائيا شبكة اتصال مؤقتة دون استخدام لأي من البنى التحتية للشبكات اللاسلكية الموجودة و كذلك عدم وجـــود إدارة مركزية لها . هناك العديد من بروتوكولات التوجيه التي تم تطويرها من قبل الباحثين و الخاصة بهذا النوع من الشبكات اللاسلكية ونظرا لطبيعة هذه الشبكات فان تأمين بروتوكولات التوجيه فيها يعد مجالا هامـــا للبحـــث . على الرغم من أن الباحثين طوروا عددا من بروتوكولات التوجيه الآمنة إلا أن استخدام هـــذه البروتوكـــولات مرهون بمدى مقاومتها للأنواع المختلفة من الهجمات و كفاءتها في الأداء. بعد تقييم هذه البروتوكولات من قبل الباحثين فان النتائج تشير إلى أنها لا تعطي الحماية الكاملة ضد الهجمات المحتملة ولها كذلك بعض المـــساوئ في أدائها.

في هذا البحث قمنا بدراسة بروتوكول توجيه جديد يدعى بروتوكول التوجيه عند الطلب و عـــن بعـــد المعتمد على الأوزان و الذي يتسم بالكفاءة و أفضل من باقي بروتوكولات التوجيه فـــي الـــشبكات اللاســـلكية العشوائية من ناحية الأداء لكنه غير آمن بالنسبة للهجمات. لذلك قمنا بتطوير بروتوكول توجيه جديد معتمد عليه و لكنه أكثر فعالية و أكثر أمنا. و قد قمنا بتحليل البروتوكول الجديد ضد الأنواع المختلفـــة و المحتملـــة مـــن الهجمات لضمان مناعته ضدها. و كذلك قمنا بإجراء العديد من اختبارات المحاكاة للبروتوكول الجديد باستخدام مقاييس اختبار الأداء الأكثر شيوعا في الشبكات اللاسلكية و ذلك لضمان كفاءته و فعاليتـــه. إن النتـــائج التـــي حصلنا عليها تشير إلى أن البروتوكول الجديد آمن و فعال بالنسبة للبروتوكولات التوجيه المستخدمة الآن.

Dedication

To the soul of my mother.

To my father.

To my brothers.

To my sisters.

And to everyone who loves me.

Acknowledgment

First of all I would like to thank Allah almighty for giving me the power and help to accomplish this research and making this work successful. Without his help nothing was possible (Alhamdulillah).

Then I am grateful to my supervisor Dr. Aiman Abu Samra for his enormous support, valuable advice, encouragement and professional assistance throughout the work of this research.

Then I would like to thank all my family members who have been constant source of motivation, inspiration and support during my whole educational life and also their guidance at each and every step.

Finally I like to thank all my friends and well to all good people for their encouragement and help.

Contents

List of Tables

List of Figures

List of Abbreviations

MANET	**Mobile Ad hoc Network**
AODV	**Ad hoc On-demand Distance Vector routing protocol**
WBAODV	**Weight-Based Ad hoc On-demand Distance Vector routing protocol**
TMR	**Throughput Maximization Routing**
SWORP	**Stable Weight-based On-demand Routing Protocol**
SAODV	**Secure Ad hoc On-Demand Distance Vector routing protocol**
REHIDAN	**Real-time Host Intrusion Detection for Ad hoc Networks algorithm**
RREQ	**Route Request packet**
RREP	**Route Reply packet**
RERR	**Route Error packet**
QoS	**Quality of Service**
HC	**Hop count**
BW	**Bandwidth**
PB	**Power of battery**
SP	**Speed**
MHC	**Max Hop count**
MPB	**Max Power of battery**
MBW	**Max Bandwidth**
DSR	**Dynamic Source Routing protocol**
SEAD	**Secure Efficient Distance Vector Routing protocol**
ARAN	**Authenticated Routing for Ad hoc Networks**
SRP	**Secure Routing Protocol**
SAR	**Security- Aware Routing Protocol**

SAKM	**Simple Ad hoc Key Management system**
ACK	**Acknowledgment**
PK	**Public Key**
SK	**Secret Key**
WREQ	**Witness Request packet**
WREP	**Witness Reply packet**
ACREQ	**Accusation Request packet**
ACREP	**Accusation Reply packet**
AC	**Accusation packet**
FAP	**Flooding Attack Prevention**
SWBAODV	**Secure Weight-Based Ad hoc On-demand Distance Vector protocol**
InfoSec	**Information Security**
DoS	**Denial-of-Service attack**
TTL	**Time To Live**
DSDV	**Destination Sequenced Distance Vector routing protocol**
TIR	**True Isolation Rate**
FIR	**False Isolation Rate**
JiST/SWAN	**Java In Simulation Time for Scalable Wireless Ad hoc Networks**
CBR	**Constant Bit Rate**
TCP	**Transmission Control Protocol**
AED	**Average End-to-End Delay**
PDF	**Packet Delivery Fraction (Ratio)**

Chapter 1

Introduction

A mobile ad hoc network (MANET) [1] [2] consists of a collection of wireless mobile nodes that are capable of communicating with each other without the use of any centralized administration or network infrastructure. The routing protocols in an ad hoc network should be able to cope well with dynamically changing topology, and nodes should exchange information on the topology of the network in order to establish routes. In general, the routing protocols of MANET can be divided into two classes: table-driven routing protocols and on-demand routing protocols. In table-driven routing protocols, every node continuously maintains the complete routing information of a network. When a node needs to forward a packet, a route is readily available. On-demand routing protocols are different from table-driven routing protocols in that on-demand routing protocols only look for routes when mobile nodes need to pass on information. Thus, on-demand routing protocols reduce much of the load required when routes are sought [3] [4] [5]. Figure (1.1) shows a typical MANET topology.

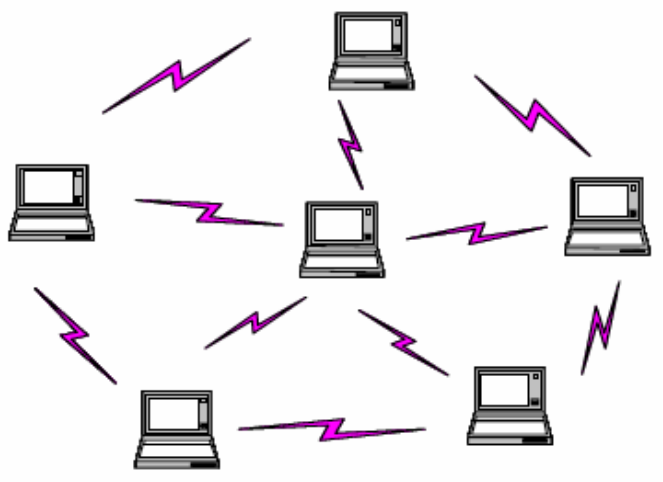

Figure (1.1): A typical mobile ad hoc network

1.1 Research Problem Statement

Although the ongoing trend is to adopt ad hoc networks for commercial uses due to their certain unique properties, the main challenge is the vulnerability to security attacks. A number of challenges like open peer-to-peer network architecture, stringent resource constraints, shared wireless medium, dynamic network topology etc. are posed in MANET. As MANET is quickly spreading for the property of its capability in forming temporary network without the aid of any established infrastructure or centralized administration, security challenges have become a primary concern to provide secure communication. Network layer is more vulnerable to attacks than all other layers in MANET. A variety of security threats are imposed in this layer. Use of secure routing protocols provides the first line of defense. So necessity of secure routing protocol is still a burning question. There is no general algorithm that suits well against the most commonly known attacks.

1.2 Research Significance

Like other networking sectors, providing a proper routing security in wireless ad-hoc networks turns out to be an important issue. Recently wireless ad-hoc networks become very popular due to their infrastructure-less characteristics and easy deployment nature. Sensitive information exchanged by the users of the devices is always susceptible to attack. Malicious tools running on the host device are often used to carry out these various attacks. So this research is very important because if we use the new proposed algorithm then all the attacks designed for routing protocols in MANET will be failed and with reasonable performance.

1.3 Research Goal

The goal of this thesis is to propose a new secure routing protocol in MANET which can be called the secured version of WBAODV routing protocol. Then the new protocol is subjected to simulation using JiST/SWAN tool and analyzed in terms of security requirements of ad hoc networks and efficiency in terms of performance metrics.

1.4 Research Purpose

The secure protocol development has become the most challenging task in securing ad hoc networks. Most of these existing protocols have been developed based on specific security scenarios. In general these existing secure routing protocols are vulnerable to some modern possible routing attacks or have weakness in their performance. So the main purpose of this research is to propose a new secure routing protocol based on WBAODV and satisfying two primary points: immunity against all modern possible attacks and efficiency to ensure its superiority to the these existing secure routing protocols in MANET.

1.5 Research Scope

MANET's Infrastructure-less topologies, communication medium and with no central administration presents a host of research areas like authentication, availability, secure routing, intrusion-detection, etc. The research approaches in MANET security can be categorized into four principal categories:

- Key management models.
- Secure routing protocols.
- Intrusion detection systems.
- Trust based models.

This thesis work focuses on secure routing protocols. The work is basically organized to propose a new secure routing protocol in MANET. Researchers developing secure routing protocols can use the result of this work as a reference.

1.6 Target Audience

This thesis addresses the readers having basic knowledge of networks and information security and who want to know about ad hoc networks and their routing protocols security. For researchers developing secure routing protocols this work is useful for further protocol development.

1.7 Approach and Procedures

Security has become a primary issue in order to provide protected communication among mobile nodes within the wireless ad-hoc network. There are many attacks that can target the ad-hoc routing protocol in which the malicious node actively interrupts the functioning of the cooperative routing mechanisms. To prevent threats or attacks and make secure communication, we begin our approach by studying these routing attacks, knowing how these attacks work and also analyzing these attacks against existing secure routing protocols in MANETs to find why they are vulnerable to these attacks. Then there are number of security goals that should be in mind and achieved before designing any kind of security architecture or application. These security goals are confidentiality, availability, integrity, authentication, non-repudiation and access control.

Then the approach is extended to thoroughly understand the issues related to secure a routing protocol for MANETs such as WBAODV routing protocol. A framework based on this understanding has to be put up to evaluate a security mechanism for WBAODV both in terms of functionalities and performance. This dual

approach emphasizes the scope and the feasibility of the evaluated security mechanism, two important parameters for an effective deployment. The design of a security mechanism has to take this framework into account in order to produce a functional secure network, with a well understood meaning for both ”functional” and ”secure”.

To accomplish the previous discussed approach, this research on securing WBAODV routing protocol has four parts. In the first part, a general as well as a context-centered study is carried out to gather information and analyze it. In the second part, results are gathered for developing a secure routing protocol based on WBAODV. Third part consists of the new protocol simulation using JiST/SWAN tool, analyzing it against most of possible modern attacks and evaluating it with the most commonly well-known ad hoc performance metrics. Fourth part is to write the final report and conclusion.

Each of the above mentioned parts are further divided into sub modules. First part includes initial module. Second part has a developing module. Third part has been divided into: simulation module, analysis module and evaluation module. Fourth part consists of finishing module. Figure (1.2) shows the flow of the research methodology.

Here is a brief of each module:

- Initial module: information gathering familiarizes with the information related to the research, implement the WBAODV routing protocol and test its performance against AODV.
- Developing module: depending on information gathered in initial module to develop and secure WBAODV.
- Simulation module: implementing the new secure protocol using JiST/SWAN tool.

- Analysis module: analyzing the new secure routing protocol against most modern possible attacks to ensure its immunity against them.
- Evaluation module: identifies the efficiency of the new secure routing protocol and compare it with MANET existing secure routing protocols.
- Finishing module: write the results obtained from the previous modules, conclusion and future work.

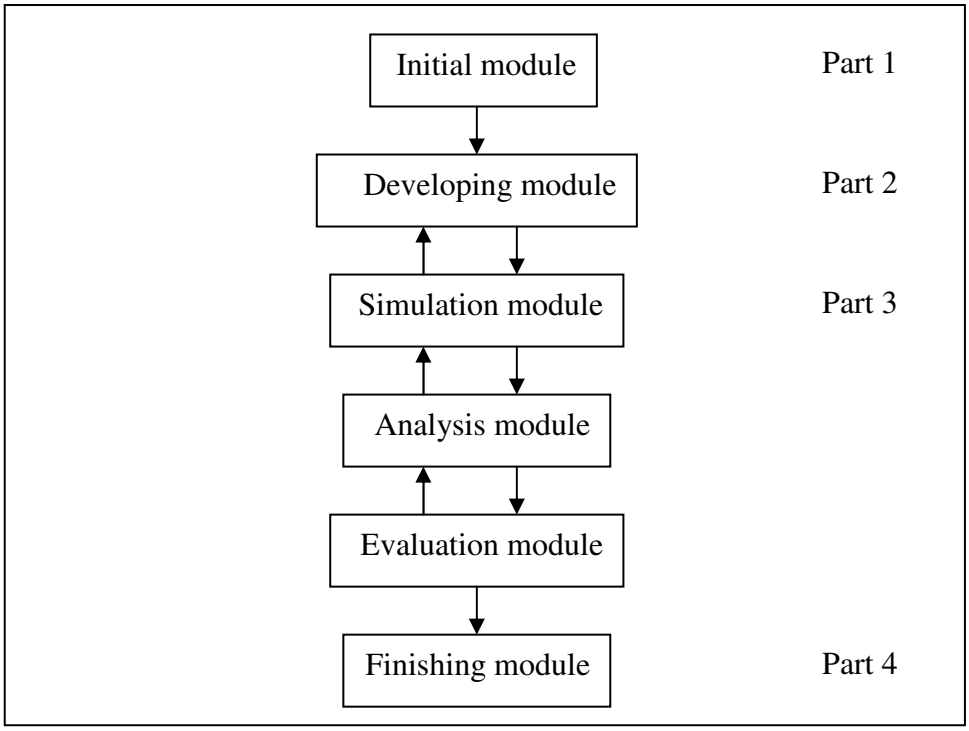

Figure (1.2): Research Methodology

1.8 Thesis Structure

There are six chapters in this thesis. The rest of the five chapters are organized as follows. Chapter 2 describes the literature review and the theoretical background for the research. Basics concepts of AODV, WBAODV and secure routing protocols in MANET are included. In chapter 3 we propose our new secure routing protocol. First we present some preliminaries of our works. Next we discuss the assumptions, notations and modifications which are needed to secure WBAODV. Then our new secure routing protocol's full description is given. Chapter 4 discuses the security analysis of our new

secure routing protocol. First we analyze our new secure routing protocol against most commonly possible routing attacks in MANET. Then we also analyze six of famous MANET's secure routing protocols against the same routing attacks and make comparison between them and our new secure routing protocol to ensure its immunity against attacks. Chapter 5 discuses the performance analysis of our new secure routing protocol. First we present some information about the JiST/SWAN simulation tool which we used to build our new secure routing protocol. Next we describe our simulation model and parameters. Then we subject our new secure routing protocol and two of famous secure routing protocols in MANET to extensive simulations with the most commonly well-known ad hoc performance metrics to ensure our new secure routing protocol's efficiency. Finally, in chapter 6, conclusions and suggestions for future work are given.

Chapter 2

Theoretical Background and Literature Review

2.1 Literature Review

In the literature there are many papers that try to enhance the performance of AODV routing protocol or to secure it against some specific attacks. The papers that enhance AODV performance are such that: In 2005 V.Sumathy, P. Narayanasamy, J.James and S.Kanimozhi have proposed a Throughput Maximization Routing (TMR) to predict the link breakage time and send a warning message to the source node of the packet and reduce the packet loss due to less energy in the node and packet loss is also reduced by providing multiple alternate routes to deliver data packets [6]. In 2005 Zheng Kai, Wang Neng and Liu Ai-fang proposed a AODV-based clustering routing protocol (called AODV-clustering) which can effectively solve scalability problem and also keep the merits of AODV [7]. In 2007 Nen-Chung Wang, Yung-Fa Huang and Jhu-Chan Chen proposed a Stable Weight-based On-demand Routing Protocol (SWORP) for MANETs. The proposed scheme uses the weight-based route strategy to select a stable route in order to enhance system performance. The weight of a route is decided by three factors: the route expiration time, the error count, and the hop count. Route discovery usually first finds multiple routes from the source node to the destination node. Then the path with the largest weight value for routing is selected [8]. In 2008 Khamforoosh, Rahmani and Sheikh Ahmadi presented a new plan in multiple paths on-demand distance vector (AODV) routing who is based on the distance of nodes from the center of the network. In this new routing algorithm, the number of dropped packets will be decreased and indeed this will happen with more balancing in the network [9].

In 2009 Shayesteh Tabatabaei and Mohammad Ali Jabraeil Jamali provided a centralized algorithm for routing in Ad hoc networks which they called Weight-Based AODV (WBAODV) routing protocol. Simulation results show that the WBAODV algorithm improves the throughput and delay significantly and also improves the network performance [10].

The papers that try to secure AODV against some specified attacks are such that: In 2001 Manel Guerrero Zapata proposed the secure version of AODV routing protocol which called "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing protocol" but this protocol is vulnerable to some possible attacks such that denial of service attack, tunneling attack and wormhole attack [11]. In 2005 Liu Jun, Li Zhe, Lin Dan and Liu Ye analyzed the potential insecurity factors in the AODV protocol and proposed a security routing protocol based on the credence model is which can react quickly when some malicious behaviors in the network are detected and effectively protects the network from some kinds of attacks and guarantees the security of ad hoc networks [12]. In 2007 Djamel Djenouri, Othmane Mahmoudi, Mohamed Bouamama, David Llewellyn-Jones and Madjid Merabti deal with securing routing protocols of mobile ad hoc networks (MANETs) against packet dropping misbehavior. More specifically, they proposed a solution to protect control packets of reactive source routing protocols against [13]. In 2009 N.Bhalaj and A.Shanmugam analyzed the blackhole attack which is one of the possible and commonest attacks in ad hoc networks. In their approach they classify nodes in to three categories based on their behavior. The extents of association between the nodes are used for the route selection [14]. In 2009 Mohammed Ibrahim, Nayera Sadek and Mohamed El-Banna addressed the flooding attack by applying multiple nodes in a simulated environment. They proposed a Real-time Host Intrusion Detection for Ad hoc Networks (REHIDAN) algorithm to identify the flooding attacker

nodes. It also takes the appropriate countermeasures to minimize the effectiveness of the attack and maintain the network performance within the accepted limits [15].

2.2 AODV Routing Protocol Overview

The Ad hoc On-Demand Distance Vector protocol (AODV) is a reactive protocol designed for ad hoc networks [16]. AODV offers low overhead, quick adaptation to dynamic link conditions and low processing and memory overhead. AODV uses a broadcast route discovery mechanism, and it relies on dynamically established routing table entries at intermediate nodes. The functions performed by AODV protocol include local connectivity management, route discovery, route table management and path maintenance. Local connectivity management may be summarized as follows. Nodes learn about their neighbors by either receiving or sending broadcast packets from or to their neighbors. Receiving the broadcast or HELLO packet from a new neighbor or failing to receive HELLO packet from a node that was previously in the neighborhood, indicates that the local connectivity has changed.

The source node initiates path discovery by broadcasting a Route Request (RREQ) packet to its neighbors. When a node receives a RREQ, in case it has routing information, it sends the Route Reply packet (RREP) back to the destination. Otherwise, it rebroadcasts the RREQ packet further to its neighbors. As the RREQ packet travels from the source to the destination it automatically sets up the reverse path for all nodes back to the source. As the RREP travels back to the source, each node along the path sets up a forward pointer to the node from which the RREP came and updates its timeout information for route entries to the source and the destination.

Each node maintains a monotonically increasing sequence number, which serves as a logical time at that node. Also, every route entry includes a destination sequence

number, which indicates the “time” at the destination node when the route was created. The protocol uses sequence numbers to ensure that nodes only update routes with “newer” ones. Doing so, we also ensure loop- freedom for all routes to a destination.

All RREQ messages include the originator’s sequence number, and its (latest known) destination sequence number. Nodes receiving the RREQ add or update routes to the originator with the originator sequence number, assuming this new number is greater than that of any existing entry. If the node receives an identical RREQ message via another path, the originator sequence numbers would be the same, so in this case, the node would pick the route with the smaller hop count (the shortest path).

If a node receiving the RREQ message has a route to the desired destination, then we use sequence numbers to determine whether this route is “fresh enough” to use as a reply to the route request. To do this, we check if this node’s destination sequence number is at least as great as the maximum destination sequence number of all nodes through which the RREQ message has passed. If this is the case, then we can roughly guess that this route is not terribly out-of-date, and we send a RREP back to the originator.

As with RREQ messages, RREP messages also include destination sequence numbers. There are so nodes along the route path can update their routing table entries with the latest destination sequence number.

Path maintenance is performed in several ways. When any node along an established path moves, so that some of the nodes become unreachable, a Route Error packet (RERR) packet is sent to affected source nodes. Whenever a Node receives RERR it looks at the Routing Table and removes all the routes that contain the bad Nodes. Upon receiving notification indicating a broken link, the source node restarts the

path discovery process, if it still needs that route [17]. Figure (2.1) shows flow chart that summarizes the action of an AODV node when processing an incoming message. HELLO messages are excluded from the diagram for brevity.

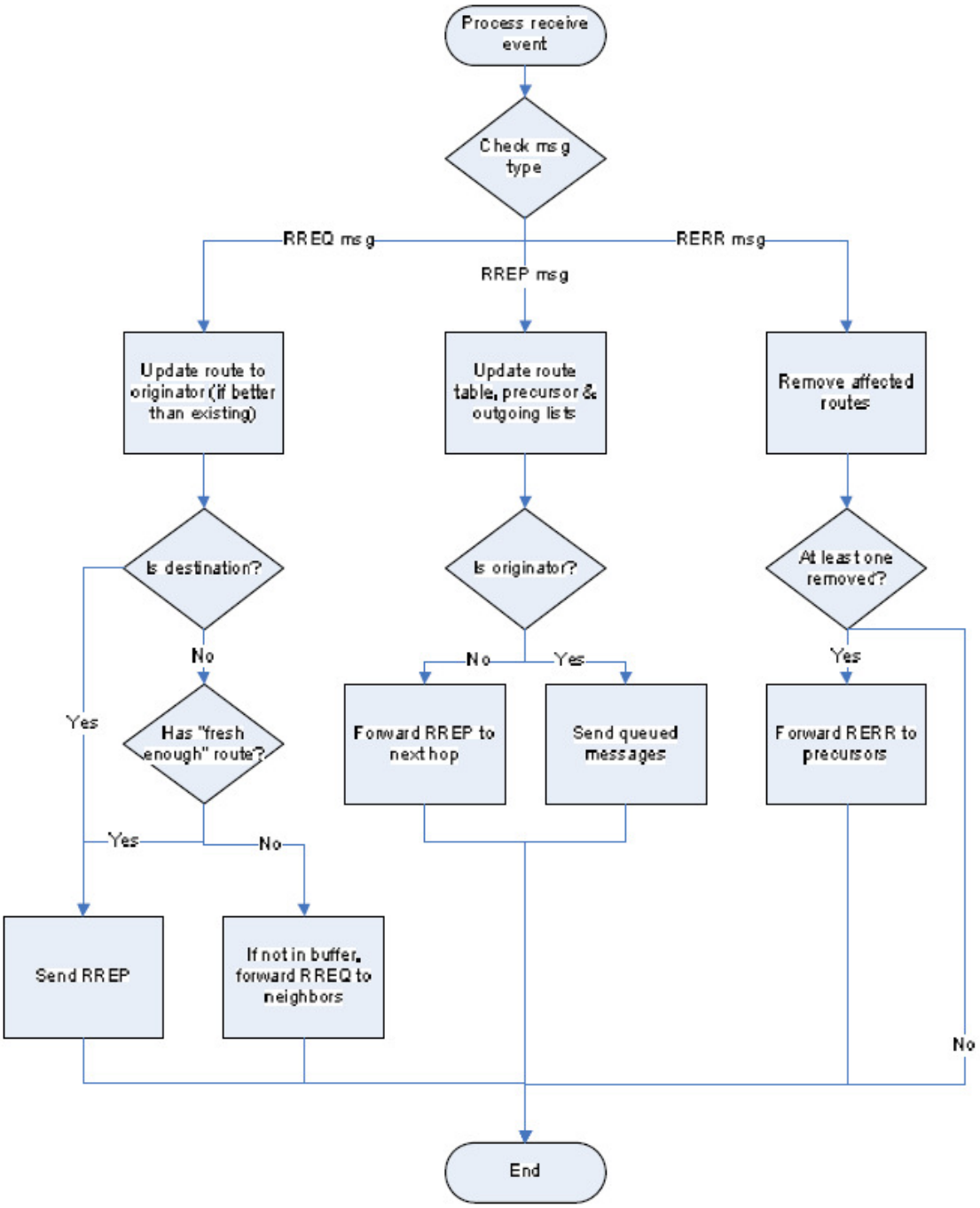

Figure (2.1): AODV Processes Flow Chart

2.3 WBAODV Routing Protocol Overview

There are two main issues in ad hoc wireless networks. The first is the Quality of Service (QoS) problem. Quality of service is very important since multimedia services become popular. Over the past few years a considerable number of studies have been made on this aspect. The other issue is the mobility problem. In MANETs, whichever routing protocols are aimed at how to find a shortest path. Due to the host's mobility in ad hoc network, a shortest path isn't necessarily the better path. If you don't consider the stability of routing path, then wireless links is easy to be broken. Many researches have been done how to enhance the networks stability. (For example, stability aware cluster routing protocol for mobile ad hoc network [18], the stable paths problem and interdomain routing [19], a reliable route selection algorithm using global position systems in mobile ad hoc networks [20]). Therefore, to enhance the networks stability a Weight-based AODV routing protocol (WBAODV)) is proposed to achieve this objective [10]. The proposed scheme uses the weight-based route strategy to select the most stable route (the route with the largest weighted value) for data transmission in order to enhance system throughput and performance.

WBAODV improves routing quality in MANETs by using the information available in the network. This idea desires for choosing a stable path for decreasing overhead for path finding, decreasing number of hops for presenting in path finding and optimized use of powerful and energetic paths [10]. There are several important parameters [10] [21] [22]:

1-Hop count (HC): this parameter as the distance (in hops) between the routers otherwise the HC is the number of hops for a feasible path. The smaller the HC is, the more reliable the routing path. The destination node D knows the HC value of the feasible paths via the hop count in the RREQ packet. As shown in figure (2.2) for Path I

(S, A, K, H, D), HC1 = 4. For Path II (S, B, E, D), HC2 = 3. For Path III (S, C, F, G, D), HC3 = 4.

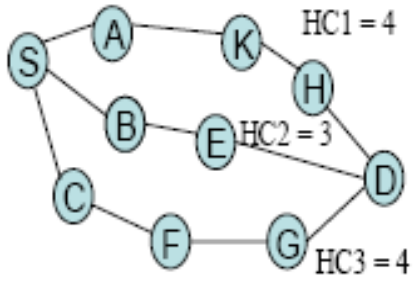

Figure (2.2): Hop count of each feasible path

2-Bandwidth metric (BW): this parameter shows, accounts necessary bandwidth for sending a file. To measure the bandwidth for a (i, j) link. This link has an available bandwidth according to following equation:

$$B\_available\ (i, j) = (1-u)*Bandwidth\ (i, j)$$

Where u is the link utilization (i.e. u = A (t)/t, A (t) is the total amount of time where the link is used by nodes during an interval of time t).

3-Power of battery (PB): With using the parameter, account necessary energy for completely sending a file or data before transforming data packages with considering the size of packages.

4-Speed (SP): this parameter shows rate of mobility for mobiles.

5-Max Hop count (MHC): is the maximum Hop count for all feasible paths.

6-Max Power of battery (MPB): is the maximum Power level of battery for mobile.

7-Max Bandwidth (MBW): this parameter shows, accounts maximum available bandwidth between two adjacent nodes.

The reliability of a feasible path is based upon four factors: the mobility of nodes, the power level of battery, the Bandwidth and the hop count. WBAODV

effectively combines all the four parameters with weighing factors F1, F2, F3 and F4, the values of which can be chosen according to the system requirements. For example, the power level of battery is very important in MANET. Thus, the weight of that factor can be made +1. The flexibility of changing the factors helps in using WBAODV to select a routing path. A larger route expiration time represents higher reliability, as do a lower error count and lower hop count [10].

The weight function in [10] is defined as an empirical mean value, where they first normalize each item and then combine these four quantities. More precisely,

$$W_i = F_1 * (SP) + F_2 * (PB/MPB) + F_3 * (HC/MHC) + F_4 * (BW/MBW)$$

Where |F1| * |F2| *|F3| * |F4| =1. For example assume that F1 = -1, F2 = +1, F3 = -1, and F4 =+1.

WBAODV Selects the route with the largest weight value among all feasible route paths to be the main routing path. Also path finding, table structure and path maintenance processes in WBAODV are like the AODV routing protocol. Figure (2.3) shows the pseudo code of WBAODV routing protocol.

Step 1: When the source S receives a packet from the transport layer in direction of destination D, it checks if a route exists to the destination.
- If it already has a route, it transmits the packet to the next hop node.
- Else, it transmits a RRREQ request.

Step 2: When a node X receives a RREQ request with a source S, a destination D and a source-sequence-number (sqn_1) then:
X calculates the weight (W_i) with the weight function.

Step 3: If the pair < S, D> exists in the reverse route entry table for node X with a weight (W_1) and a source- sequence-number denoted (sqn_2) then:

- If ($W_i > W_1$ and $sqn_1=sqn_2$) or ($sqn_1 > sqn_2$) then:
  X updates this reverse route entry table
  - If (X # D)
    X broadcasts the RREQ request up to date
  - Else
    X sends a RREP request
- Else
  X discards the RREQ request

Step 4:
-If the condition in step 3 doesn't satisfied then:
Go to step 5.
- Else go to step 6.
Step 5: X creates a new pair < S, D > in its reverse route entry table with the weight equal to W_i and a source-sequence-number equal to sqn_1
-If (X = D)
X sends a RREP request
- Else
X broadcasts the RREQ request up to date
Step 6: When a node X receives a RREP request from node Y with a source S, a destination D, a weight W_1, and a source-sequence-number sqn_1 then:
Go to step 7.
Step 7: If the pair < S, D > exists in the routing table for node X with a weight W_2 and a source-sequence-number denoted sqn_2 then:
-If (W1 > W2 and sqn1=sqn2) or (sqn1 > sqn2)
X updates the routing table with the next hop Y
• If (X # S)
X forwards the RREP to the previous node
-Else
X discards the RREP
Step 8:
-If the condition in step 7 doesn't satisfied then:
X creates a new tuple in its routing table with the next hop Y
•If (X # S)
X forwards the RREP to the previous node

Figure (2.3): WBAODV routing protocol pseudo code

According to the results in [23], WBAODV outperforms Dynamic Source Routing (DSR) and AODV routing protocols in performance especially in the high mobility environment.

2.4 MANET Secure Routing Protocols and SAODV Security Mechanism

In Mobile Ad hoc Networks (MANET) much of the research has been done focusing on the efficiency of the network. There are quite a number of routing protocols that are excellent in terms of efficiency. But the security requirements of these protocols changed the situation and a more detailed research is currently underway to develop

secure ad hoc routing protocols [24] [25]. MANETs are extremely vulnerable to attacks [26] [27] [28] due to their dynamically changing topology, absence of conventional security infrastructures and open medium of communication, which, unlike their wired counterparts, cannot be secured. To address these concerns, several secure routing protocols have been proposed: Secure Efficient Distance Vector Routing (SEAD) [29], Ariadne [53], Authenticated Routing for Ad hoc Networks (ARAN) [47], Secure Ad hoc On-Demand Distance Vector Routing (SAODV) [11], Secure Routing Protocol (SRP), and Security- Aware Routing Protocol (SAR). Although researchers have proposed several secure routing protocols, their resistance towards various types of security attacks and efficiency are primary points of concern in implementing these protocols. After the evaluation of these protocols in [30] the results refer to that they do not give complete protection against possible attacks or have some disadvantages on their performance. Hence, there is a need for developing a new secure routing protocol with efficient performance.

In an ad hoc network, from the point of view of a routing protocol, there are two kinds of messages: the routing messages and the data messages. Both have a different nature and different security needs. Data messages are point-to-point and can be protected with any point-to-point security system (like IPSec). On the other hand, routing messages are sent to immediate neighbors, processed, possibly modified, and resent.

Another consequence of the nature of the transmission of routing messages is that, in many cases, there will be some parts of those messages that will change during their propagation. This is very common in Distance-Vector routing protocols, where the routing messages usually contain a hop count of the route they are requesting or providing. Therefore, in a routing message one could distinguish between two types of

information: mutable and non-mutable. It is desired that the mutable information in a routing message is secured in such a way that no trust in intermediate nodes is needed. Otherwise, securing the mutable information will be much more expensive in computation, plus the overall security of the system will greatly decrease. Moreover, as a result of the processing of the routing message, a node might modify its routing table. This creates the need for the intermediate nodes to be able to authenticate the information contained in the routing messages (a need that does not exist in point-to-point communications).

SAODV addresses the problem of securing a MANET network. SAODV is an extension of the AODV routing protocol that can be used to protect the route discovery mechanism providing security features like integrity, authentication and non-repudiation.

SAODV assumes that each ad hoc node has a signature key pair from a suitable asymmetric cryptosystem. Further, each ad hoc node is capable of securely verifying the association between the address of a given ad hoc node and the public key of that node. Achieving this is the job of the Simple Ad hoc Key Management (SAKM) which is a key management system that allows the nodes of an ad hoc network to use asymmetric cryptography with zero configurations [31]. Two mechanisms are used in SAODV to secure the routing messages:

1-Digital signatures: to authenticate the non-mutable fields of the messages. They also provide an end-to-end authentication and node-to-node verification of these messages. The underlined process is relatively simple. The source node digitally signs the route request packet (RREQ) and broadcasts it to its neighbors. When an intermediate node receives a RREQ message, it first verifies the signature before creating or updating a reverse route to its predecessor. It then stores or updates the route only if the signature is

verified. A similar procedure is followed for the route reply packet (RREP). As an optimization, intermediate nodes can reply with RREP messages, if they have a “fresh enough” route to the destination. Since the intermediate node will have to digitally sign the RREP message as if it came from the destination, it uses the double signature extension described in this protocol. There are many digital signature methods available like: RSA, DSA and ElGamal [31].

2- Hash chains: to secure the hop count information (the only mutable information in the messages). This is because for the non-mutable information, authentication can be performed in a point-to-point manner, but the same kind of techniques cannot be applied to the mutable information. During the route discovery process, the source node first selects a random seed number and sets the Maximum Hop-count (MHC) value. By using a hash function h, the source computes the hash value as h (seed) and Top_Hash as h^{MHC} (seed). When an intermediate node receives an RREQ message, it checks whether the value of Top_Hash is equal to $h^{MHC-Hop\_Count}$ (Hash). If so, it will assume that the hop count has not been altered. Before rebroadcasting the RREQ to the neighboring nodes, the intermediate node will increment the hop-count field by one in the RREQ header and also compute the new Hash value by hashing the old value (i.e., h(Hash)). Except for the hop-count field and h^{hop_count} (seed), all other fields of the RREQ are non-mutable and therefore can be authenticated by verifying the signature in the RREQ. When the destination node receives an RREQ, it generates an RREP in the same way. SAODV can also allow an intermediate node to generate an RREP by using double signature extension. There are many hash functions are available like: MD2, MD5, SHA1, SHA256, SHA384 and SHA512 [32].

Route error messages are protected in a different manner because they have a big amount of mutable information. In addition, it is not relevant which node started the

route error and which nodes are just forwarding it. The only relevant information is that a neighbor node is informing another node that it is not going to be able to route messages to certain destinations anymore. Therefore, every node (generating or forwarding a route error message) uses digital signatures to sign the whole message and that any neighbor that receives verifies the signature [31].

2.5 Control Packets Dropping Prevention Scheme

In this section we present securing routing protocols of mobile ad hoc networks (MANETs) against packet dropping misbehavior. More specifically, we overview a solution to protect control packets of reactive routing protocols against. Most current proposals focus on data packets. Nonetheless, dropping control packets may be beneficial for selfish nodes and malicious ones as well. For example, simply by dropping RREQ packets a selfish node could exclude itself from routes and thereby avoid receiving data packets to forward. Similarly, a malicious node could drop RERR packets to keep the use of failed routes, potentially resulting in a denial of service. In the following we give some details of the solution in [13] to monitor the forwarding of control packets, judge the monitored nodes, and isolate the detected misbehaving nodes.

2.5.1 Monitoring Directed Packets

The approach suggests to use to monitor the forwarding of directed routing control packets (RREP, RERR) needs to be implemented with a source routing protocol. Each node A monitors its successor B in the route and checks whether this latter forwards to C each packet it provides, such that C is B's successor in the route and A could be either the source or any intermediate node. This process is repeated on each couple of hops until reaching the final destination. The solution uses a special kind of feedbacks called two-hop ACK that travels two hops [33]. Node C acknowledges

packets sent from A by sending this latter via B a two-hop ACK. To ensure authentication of two-hop ACK packets an asymmetric cryptography-based strategy is used. Node A generates a random number and encrypts it with C's public key (PK), and then appends it in the packet's header. When C receives the packet it retrieves the number, decrypts it using its secret key (SK), encrypts it using A's PK, and puts it in a two-hop ACK it sends back to A via B. When A receives the ACK it decrypts the random number and checks whether it matches with the one it has generated, in order to validate B's forwarding regarding the appropriate packet. However, if B does not forward the packet A will not receive the two-hop ACK, and it will be able to detect this dropping after a timeout. This strategy requires a key distribution mechanism enabling a security association between each pair of nodes. Note that the same keys could be employed for other security purposes at the other layers. As soon as the monitor node detects that the number of packets dropped by the monitored node exceeds a defined threshold, it considers this latter as misbehaving and proceeds to its isolation. Note that dropping RREPs (respectively RREQs) prevents a selfish node from being included in routes, while dropping RERRs allows a malicious node to launch a denial of service attack by preventing the destruction of broken routes. Also, note that the overhead is not an important issue for this kind of packets, since their number is low [13].

2.5.2 Monitoring Broadcast Packets

For RREQs packets (which are broadcast), each node monitors every RREQ it forwards or launches as a source. The monitoring starts from the reception of the RREQ (or its launch if the node is the source) and ends after a timeout from its retransmission. For each RREQ, the transmitter monitors all its neighbors. It should either receive (or overhear) the RREQ or a RREP from every neighbor, except the node from which it received the RREQ if the node is not the source. If no one of these packets is received

from a neighbor B, then the monitor notices a packet dropping for B. When a node observes that another node B drops more than the configured threshold number of packets it judges B as misbehaving, and tries to isolate it as we will see later [13].

2.5.3 Redemption

To get over false detections that may occur due to nodes mobility and channel conditions, they present a redemption strategy for both kinds of packets. The aim is to allow a well-behaving node improving its reputation and tolerance threshold after it has been observed to drop packets due to mobility or collisions. This can be achieved by decreasing the number of packets considered dropped each time it is perceived to correctly forward packets. The pace of decreasing is not inevitably 1, but should be < 1 to prevent nodes from abusing this redemption. That is, forwarding one packet does not decrease the number of packets considered dropped by one. If the pace is m/n (such that $m,n \varepsilon N, m < n$), then forwarding n packets decreases the number by m [13].

2.5.4 Isolation

After judging a node as misbehaving, the detector attempts to isolate it. Isolating a misbehaving node means: do not route packets through it, to avoid losing them, and do not forward packets for it, to punish it. A node A that judges some other node B as misbehaving should not punish it unilaterally, but must ensure that this will be done by all nodes. This is because when A unilaterally punishes B; the others could consider A as misbehaving when they realize that it does not forward packets for B. In social life, a person that accuses another must show proof. One possible way to prove the accusation is to get witnesses against the accused person. Similarly, to isolate a detected node they present the use of a testimony-based protocol [34], already used with data packets. Upon a detection, the detector informs nodes in its neighborhood about the dropper (the accused), and asks for witnesses by broadcasting a WREQ (Witness REQuest) packet. It

also puts the detected node ID in a special set we call a suspicious set. Each node receiving the WREQ investigates the issue as follows:

For directed packets: The receiver of WREQ immediately sends a signed WREP (Witness REPly) packet to the accuser if its suspicious set includes the accused node (denoted by B). Otherwise, if it has not enough experience with the accused node, and if B is its neighbor then it asks the successor of this latter whether it has received packets forwarded from it, by sending an ACREQ (ACcusation REQuest) packet, using a route that does not include B. But first, in order to avoid false accusations, the investigator should ensure that the accuser has really sent a packet to B to be forwarded to the appropriate successor. One possible way to do this is to check whether such a packet has been recently overheard, using the promiscuous mode. The node also should check whether B has sent the accuser an ACK just after overhearing the data, to ensure that the former has really received the packet and that the latter does not impress it. If B's successor has not recently received any packet forwarded from B, it sends a signed ACREP (ACcusation REPly) packet to the investigator, then this latter testifies for the accusation and sends the accuser a signed WREP (Witness REPly) packet [13].

For broadcast packets: In this case the node, if it is a neighbor of B, merely checks whether it has recently received (respectively overheard) either any RREQ forwarded from this node, or a RREP originated from it. To do this, each node keeps the RREQs and RREPs it receives in a buffer for a short time. If neither RREQ nor RREP have been received then it testifies for the accusation and sends the accuser a signed WREP (Witness REPly) packet. But it must first ensure that the accuser node has really recently sent out a RREQ, by checking in its buffer [13].

When the detector collects k validation from its neighbors, with at least one provided by direct experience (without asking the successor of B), it broadcasts in the

network an accusation packet (AC) containing signatures of all the validating nodes. The requirement of at least one direct witness aims at mitigating wrong accusations caused by false testimonies. Each node receiving such a valid accusation isolates the guilty. Otherwise, if the detector fails to collect k validation then it does not punish the detected node, but keeps it in the suspicious set and could avoid sending its own packets through it [13].

2.6 Flooding Attack Prevention Scheme

In this section, we present the Ad Hoc Flooding Attack, which results in denial of service when used against all on-demand ad hoc networks routing protocols. In this attack, the attacker either broadcasts a lot of Route Request packets for node ID who is not in networks so as to congest in links. To defend routing protocols against the Ad Hoc Flooding attack, we present a generic secure component, called Flooding Attack Prevention (FAP), which is a set of generic mechanisms that together defend against the Ad Hoc Flooding Attack. The method of neighbor suppression is used to prevent RREQ Flooding Attack. Mobile ad hoc networks are multi-hop wireless networks, and the node sends and receives packets through its neighbor nodes. If all neighbor nodes around the node refuse to forward its packets, the node can not communicate with the other nodes in mobile ad hoc networks. The node has been isolated from the network in practice even if it is still in the networks in location [35]. Figure (2.4) shows a topology of mobile ad hoc network. The node H communicates with the other nodes through node D, F, G and I. If the neighbor nodes D, F, G and I refuse to receive packets from node H, node H can not send any packet to the other nodes.

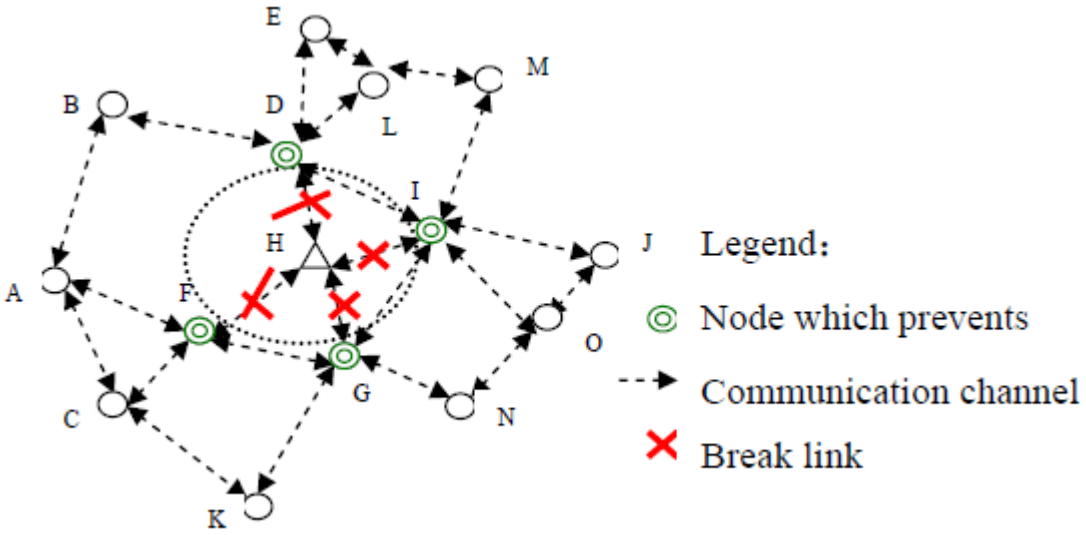

Figure (2.4): Neighbor nodes isolate the flooding attacker (node H).

The main idea of neighbor suppression is that each neighbor calculates the rate of RREQ originated by intruder. If the rate exceeds some threshold, all neighbors will not receive and forward packets from intruder. They define two tables in every node: Rate_RREQ and Flooding_Blacklist. The table of Rate_RREQ records the rate of RREQ which every neighbor node originates, and does not record times of forwarded RREQ. The Rate_RREQ has two columns: Node_ID and RREQ_time. Node_ID includes all neighbor nodes ID. RREQ_time records times which neighbor node originates RREQ [35]. The process is Algorithm 1 as shown in figure (2.5).

```
Algorithm 1. calculate time of RREQ
Step1. received a RREQ;
Step2. if the RREQ is forwarded then quit;
Step3. look up node ID who send the RREQ in the table of Rate_RREQ;
Step4. find node ID and RREQ_time:=RREQ_time+1;
```

Figure (2.5): FAP Algorithm 1.

To calculate the rate of RREQ and find the intruder, Algorithm 2 is run one time every second [35] as shown in figure (2.6).

```
Algorithm 2. find the intrusion
    For every item of Rate_RREQ do
        If RREQ_time > threshold then put Node_ID into Blacklist and RREQ_time:=0;
        Else RREQ_time:=0;
```

Figure (2.6): FAP Algorithm 2.

Because RREQ_time sets up 0 every second, it can stand for rate which every neighbor node originates. If the time exceeds the threshold, we may make a judge that it is intruder. When node receives a packet, node firstly looks up source ID of packet. If source ID is in Blacklist, node directly discards the packet. If source ID is not in Blacklist, node disposes the packet by normal process. The threshold is the maximum of originating RREQ in a period time, such as 1 second. If the frequency of originating RREQ of the attacker exceeds the threshold, the node will not receive the RREQ from the attacker any more [35]. To clarify, we take node H and its neighbor node D, I, F, G for example in figure (2.4). If the frequency which node H originates RREQ exceeds the threshold, node F will deny the RREQ packets from node H. similarly, node D, I, G will deny the RREQ packets form node H. As a result, the Ad Hoc Flooding Attack from node H is prevented by its neighbor nodes.

2.7 Wormhole Attack Prevention using Temporal Leash

In this section, we introduce the wormhole attack, a severe attack in ad hoc networks that is particularly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems. For

example, most existing ad hoc network routing protocols, without some mechanism to defend against the wormhole attack, would be unable to find routes longer than one or two hops, severely disrupting communication.

The notion of a packet leash is considered as a general mechanism for detecting and thus defending against wormhole attacks. A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. There are two types of packet leashes: geographical leashes and temporal leashes. A geographical leash ensures that the recipient of the packet is within a certain distance from the sender. A temporal leash ensures that the packet has an upper bound on its lifetime, which restricts the maximum travel distance, since the packet can travel at most at the speed of light. Either type of leash can prevent the wormhole attack, because it allows the receiver of a packet to detect if the packet traveled further than the leash allows [36].

To construct a temporal leash, in general, all nodes must have tightly synchronized clocks, such that maximum difference between any two nodes' clocks is δ. The value of the parameter δ must be known by all nodes in the network, and for temporal leashes, generally must be on the order of a few microseconds or even hundreds of nanoseconds. Although the general requirement for time synchronization is indeed a restriction on the applicability of temporal leashes, for applications that require defense against the wormhole attack, this requirement is justified due to the seriousness of the attack and its potential disruption of the intended functioning of the network [36].

To use temporal leashes, when sending a packet, the sending node includes in the packet the time at which it sent the packet, t_s; when receiving a packet, the receiving node compares this value to the time at which it received the packet, t_r. The receiver is thus able to detect if the packet traveled too far, based on the claimed transmission time

and the speed of light. Alternatively, a temporal leash can be constructed by instead including in the packet an expiration time, after which the receiver should not accept the packet; based on the allowed maximum transmission distance and the speed of light, the sender sets this expiration time in the packet as an offset from the time at which it sends the packet. The expiration time can be expressed as:

$$t_e = t_s + L / c - \Delta$$

Where t_e: packet expiration time, t_s: packet sent time, c: propagation speed of wireless signal, L: maximum allowed travel distance; $L > L_{min} = \Delta * c$ and Δ: maximum clock difference between two nodes. As with a geographical leash, a regular digital signature scheme or other authentication technique can be used to allow a receiver to authenticate a timestamp or expiration time in the received packet [36].

Chapter 3

Secure Weight-Based Ad hoc On-demand Distance Vector (SWBAODV) Routing Protocol

In this chapter we propose our new secure routing protocol which we called SWBAODV. It is based on WBAODV [10] and uses the same stable weight-based routing strategy. We secure WBAODV by adding to it some security primitives and mechanisms to enhance the immunity against various attacks. In chapter 2 we introduced general security solutions and mechanisms which are proposed to protect MANET routing protocols against certain attacks, but to apply these general solutions to WBAODV we need some assumptions and modifications to it. After doing the required assumptions and modifications, SWBAODV is obtained.

3.1 Assumptions, Notations and Modifications to WBAODV

In this sub section we mention the needed assumptions and modifications that are used in SWBAODV:

1. As SAODV the SWBAODV will use the asymmetric cryptography concepts, so each node in the network will have two keys: one private (secret) and another is public.
2. As SAODV there will be Simple Ad hoc Key Management (SAKM) which is a trusted key management system that allows the nodes of an ad hoc network to use asymmetric cryptography with zero configurations. Each ad hoc node is capable of securely verifying the association between the address of a given ad hoc node and the public key of that node through SKAM, so it will be always available.

3. SWBAODV will secure the routing messages only.
4. In RREQ packet the SWBAODV will set the D flag (Destination only flag) by 1 in the RREQ packet header to indicate that only the destination will respond to this RREQ. The objective of this step is to meet with stable weight-based routing strategy that states that the intermediate nodes shouldn't respond to RREQ even if they already know the fresh route to the destination in their routing table. Instead they are forced to forward the RREQ to let it arrives to the destination that will enable it to compute the weights of the complete paths and select the one with maximum weight. Also another benefit of this step is to reduce the processing overhead because the intermediate nodes will not use the double signatures which consumes high amount of power and take a long time to complete which at the end will enhance the performance. Figure (3.1) shows the standard AODV RREQ message format.

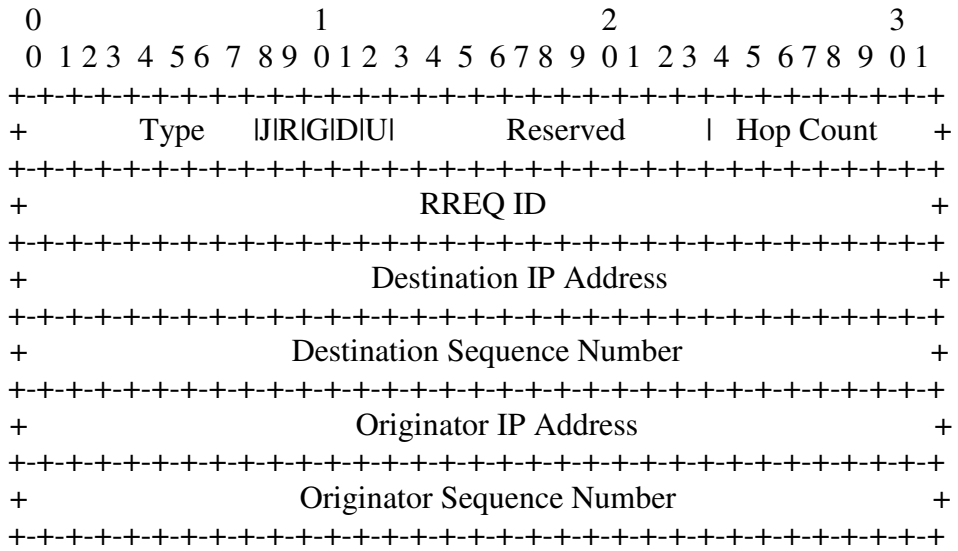

Figure (3.1): AODV Route Request (RREQ) message format

5. SWBAODV will use digital signatures with timestamps by using one of the available digital signature methods to authenticate the non-mutable fields of the routing messages, providing an end-to-end authentication, node-to-node

verification of routing messages, message integrity, message validation and as a part of temporal leash concept which is described in section 2.7.

6. SWBAODV will use hash chains to secure the hop count information (the only mutable information in the RREQ message) by using one of the available hash functions.
7. SWBAODV will sign the whole REER and HELLO massages without using hash chains.
8. When the destination node receives the first RREQ packet, it will wait for a certain time to enable itself to receive other possible RREQ packets from other possible feasible paths. Then the destination node will compute the weight for each feasible path using the weight function which described in section 2.3. Afterwards the destination node will select the path with the maximum weight value as the main data transmission routing path among all feasible paths. Finally the destination node will send a RREP packet to the source node along the main routing path.
9. We add a new field to RREQ packet which we called *Precursor_Id* to contain the previous node's IP address for the node that forwarded the RREQ packet. For example in figure (3.2): when node B receive the RREQ packet from node A, it will read the IP address of the previous node of A from the *Precursor_Id* field in the RREQ packet and store it in special table. Then node B will put the IP address for node A in this field and forward the RREQ packet to C. Similarly node C will save the IP address of A in the special table and put the IP address of B in the *Precursor_Id* field and forward the RREQ packet to its neighbors and so on. Figure (3.3) shows the SWBAODV RREQ message format.

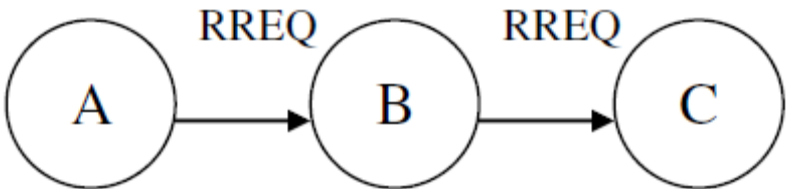

Figure (3.2): Forwarding RREQ packet in SWBAODV

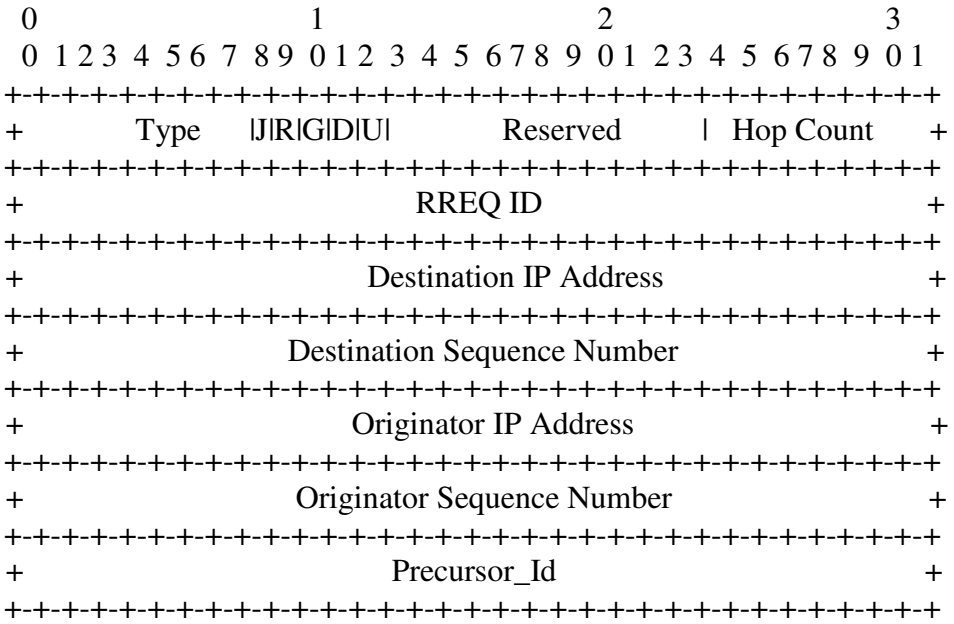

Figure (3.3): SWBAODV Route Request (RREQ) message format

10. Every node in the network will create a new table which we called *Monitoring_Table* that has four columns. These columns are SID: Source's IP address for the RREQ, DID: Destination's IP address for the RREQ, PRE_NODE_ID: the Precursor node's IP address which forwarded this RREQ, PREV_PRE_NODE_ID: the Previous node's IP address for the Precursor node that forwarded this RREQ. When a node receives a RREQ packet it adds or updates the entry for the pair <Source, Destination> in its *Monitoring_Table*. This for purposes of control packet dropping prevention scheme which is described in section 2.5. Every node will use this table to keep track of its successor nodes to monitor them when forwarded RREP or RERR packets to

them. Figure (3.4) shows the node C's *Monitoring_Table* entry for the RREQ packet in figure (3.2).

SID	DID	PRE_NODE_ID	PREV_PRE_NODE_ID
S	D	B	A

Figure (3.4): Node C's Monitoring_Table entry

11. When the source node originates the RREQ packet, it leaves the *Precursor_Id* field empty because no node is previous of it and when its neighbor receive this RREQ, they leave PREV_NODE_ID column empty in their *Monitoring_Table* because no need to monitor the source node which is the final node that will receive the RREP or REER packets. Then source's neighbors put the source's IP address in the *Precursor_Id* field of the RREQ and broadcast it to their neighbors. Then the process continues normally as illustrated in control packets dropping prevention scheme and steps 9 and 10.
12. The monitoring process doesn't include Hello packets because every node only sends or receives Hello packets to or from its neighbors.
13. Every node in the network will create a new list which we called *Suspicious_List* that will contain all suspicious nodes that drop control packets for the node that create this list. This list will be used in control packet dropping prevention scheme which is described in section 2.5.
14. SWBAODV will use some special packets like: Two-hop ACK, WREQ (witness request), WREP (witness reply), ACREQ (accusation request), ACREP (accusation reply) and AC (accusation packet). These packets are used as part of the control packet dropping prevention scheme which is described in section 2.5.
15. Every node will create two new tables: *Rate_RREQ* and *Flooding_Blacklist*. The table of *Rate_RREQ* records the rate of RREQ which every neighbor node

originates, and does not record times of forwarded RREQ. The *Rate_RREQ* has two columns: Node_ID and RREQ_time. Node_ID includes all neighbor nodes ID. RREQ_time records times which neighbor node originates RREQ. *Flooding_Blacklist* will contain all nodes that try to flood the network with RREQ packets and detected by the node that create this table. These new tables will be used in flooding attack prevention scheme described in section 2.6

16. SWBAODV will use temporal leash concept which is described in section 2.7 to prevent wormhole and tunneling attacks.
17. In temporal leash maximum clock error (Δ) must be known by all nodes in the network and be on the order of microseconds or hundreds of nanoseconds.

3.2 SWBAODV Routing Algorithm

The functions performed by SWBAODV protocol include local connectivity management, route discovery, route table management and path maintenance.

3.2.1 Local Connectivity Management Process

It may be summarized as follows. Nodes learn about their neighbors by either receiving or sending broadcast packets from or to their neighbors. At periodic intervals each node signs the whole HELLO message with timestamp and broadcasts it to its neighbors. Also when a node receives HELLO messages from its neighbors; it first will verify the signature to authenticate the sender and validation of the HELLO message, if it correct then the node will check HELLO message for tunneling or wormhole attack by using temporal leash concept, if the HELLO message isn't tunneled then the node will add or update the entries in its routing table if needed. Receiving the broadcast or HELLO from a new neighbor or failing to receive HELLO packets from a node that was previously in the neighborhood, indicates that the local connectivity has changed.

3.2.2 Route Discovery and Routing Table Management Processes

The following figure (3.5) shows the pseudo code of these processes in SWBAODV routing protocol.

Step 1: When the source S receives a packet from the transport layer in direction of destination D, it checks if a route exists to the destination.
- If it already has a route, it transmits the packet to the next hop node.
- Else:
  - S generates a RREQ packet.
  - S signs the RREQ with timestamp.
  - S broadcasts the RREQ to its neighbors.
  - S monitors its neighbors to verify that they forwarded the RREQ and isolates the suspicious nodes.

Step 2: When a node X receives a RREQ request with a source S, a destination D and a source-sequence-number (sqn_1) then:
- X verifies the signatures of the RREQ to authenticate the sender and discards it if it spoofed.
- X verifies the timestamp of the RREQ to validate it and discards it if it old.
- X computes the expiration time of RREQ to check it for tunneling or wormhole attack and discards it if it tunneled.
- X computes the weight (W_i) of the RREQ using the weight function.
- X looks up in its reverse route entry table.

Step 3: If the pair < S , D> exists in the reverse route entry table for node X with a weight (W_1) and a source- sequence-number denoted (sqn_2) then:
- If ($W_i > W_1$ and $sqn_1=sqn_2$) or ($sqn_1 > sqn_2$) then:
  - If (X # D) then:
    * X updates this reverse route entry table.
    * X increments the HOP_COUNT field by one.
    * X computes a new hash.
    * X puts the precursor node's IP address in *Precursor_Id* field of the RREQ.
    * X maintains its Monitoring_Table entry for the pair <S,D>.
    * X signs the RREQ with timestamp.
    * X broadcasts the RREQ packet up to date.
    * X monitors its neighbors to verify that they forwarded the RREQ and isolates the suspicious nodes.
    * If (precursor node= S) then:
      - ❖ X monitors S to prevent flooding attack and isolates S if it an attacker.
  - Else:
    * D waits for T time to receive all other possible RREQ packets for this pair <S,D>.
    * D compares the weights of each feasible path and selects the path with the maximum weight as main routing path.
    * D maintains its Monitoring_Table entry for the pair <S,D>.
    * D generates the RREP packet.
    * D signs the RREP with timestamp.

* D sends the RREQ packet back to S.
* D monitors its successor to verify that it forwarded the RREP and isolates the suspicious nodes.

-Else:

• X discards the RREQ packet.

Step 4:

-If the condition in step 3 doesn't satisfied then:

Go to step 5.

- Else go to step 6.

Step 5: X creates a new pair < S, D > in its reverse route entry table with the weight equal to W_i and a source-sequence-number equal to sqn_1 and do as step 3.

Step 6: When a node X receives a RREP request from node Y with a source S, a destination D, a weight W_1, a source-sequence-number sqn_1 then:

- X verifies the signatures of the RREP to authenticate the sender and discards it if it spoofed.
- X verifies the timestamp of the RREP to validate it and discards it if it old.
- X computes the expiration time of RREP to check it for tunneling or wormhole attack and discards it if it tunneled.
- X looks up in its routing table.

Step 7: If the pair < S, D > exists in the routing table for node X with a weight W_2 and a source-sequence-number denoted sqn_2 then:

-If ($W_1 > W_2$ and $sqn_1=sqn_2$) or ($sqn_1 > sqn_2$)

• If (X # S)

* X updates its routing table with the next hop Y
* X signs the RREP with timestamp.
* X forwards the RREP to the previous node
* X monitors its successor to verify that it forwarded the RREP and isolates the suspicious nodes.

• Else:

* S updates its routing table with the next hop Y.
* S starts to send data packets to the D through the main routing path.

-Else

• X discards the RREP packet.

Step 8:

-If the condition in step 7 doesn't satisfied then:

• X creates a new pair < S, D > in its routing table with the next hop Y and do as step 7.

Figure (3.5): SWBAODV routing protocol pseudo code

As shown in figure (3.5) they may be summarized as follows:

1- When a source node (S) wants to send a message to destination node (D) that hasn't a route to it in its routing table. The node first save the data message in the queue, then generate a route request (RREQ) packet, set D flag in the packet

header by one, hash a random seed number as TOP_HASH, set Maximum Hop Count field, set HOP_COUNT field by zero, sign the RREQ packet with timestamp and finally initiates path discovery by broadcasting the RREQ to its neighbors. At the same time S will monitor its successor nodes and verifies that these nodes forwarded the RREQ packet by using the control packet dropping prevention scheme. This scheme will monitor, detect and isolate the suspicious nodes by adding them to its *Suspicious_List*.

2- When an intermediate node (X) receive a RREQ packet, X first verifies the signature to authenticate the sender and validation of the RREQ packet, if it correct then X will check RREQ packet for tunneling or wormhole attack by using temporal leash concept, if the RREQ packet isn't tunneled then X computes the weight (W_i) for RREQ packet, read the RREQ sequence number (seq_i) and check its reverse route entry table.

3- If there an entry for pair <S,D> with weight W_1 and sequence number seq_1 then X checks if ($W_i > W_1$ and $seq_i = seq_1$) or ($seq_i > seq_1$) then X will update its reverse route entry for that pair, increments the HOP_COUNT field, computes a new hash , puts the precursor node's IP address in *Precursor_Id* field, maintains its Monitoring_Table entry for the pair <S,D>, signs the RREQ with timestamp and finally broadcasts the RREQ packet to its neighbors. If the previous condition doesn't satisfy then X will discard the RREQ packet. At the same time X will monitor its successor nodes and verifies that these nodes forwarded the RREQ packet by using the control packet dropping prevention scheme. This scheme will monitor, detect and isolate the suspicious nodes by adding them to its *Suspicious_List*. Also if the precursor node that forwarded RREQ packet to X is

S then X will use the FAP scheme to prevent flooding attack by isolate the attacker by adding it in its *Flooding_Blacklist*.

4- If X doesn't find any existing entry then it will create a new entry for pair <S,D> in its reverse routing entry table with weight equal to W_i and sequence number equal to seq_i. Then X increments the HOP_COUNT field, computes a new hash , puts the precursor node's IP address in *Precursor_Id* field, maintains its Monitoring_Table entry for the pair <S,D>,signs RREQ with timestamp and broadcasts the RREQ packet to its neighbors. At the same time X will monitor its successor nodes and verifies that these nodes forwarded the RREQ packet by using the control packet dropping prevention scheme. Also if the precursor node that forwarded RREQ packet to X is S then X will use the FAP scheme to prevent flooding attack by isolate the attacker by adding it in its *Flooding_Blacklist*.

5- When the destination node (D) receive the RREQ packet it will first verifies the signature to authenticate the sender and validation of the RREQ packet, if it correct then D will check RREQ packet for tunneling or wormhole attack by using temporal leash concept, if the RREQ isn't tunneled then D will wait for certain time to receive other possible RREQ packets, discards any RREQ that is tunneled, computes the weight for each remained feasible path using the weight function, selects the path with maximum weight as the main routing path, maintains its *Monitoring_Table*, generates RREP packet , signs it with timestamp and finally sends it in the reverse path back to S. At the same time D will monitor its successor node and verifies that this node forwarded the RREP packet by using the control packet dropping prevention scheme.

6- When an intermediate node (X) receive a RREP packet from a node Y, it first verifies the signature to authenticate the sender and validation of RREP packet, if it correct then X will check RREP for tunneling or wormhole attack by using temporal leash concept, if the RREP isn't tunneled then X will check its routing table.

7- If there an entry in its routing table for pair <S,D> then X will update its routing table for that pair with next hop Y, signs the RREP with timestamp and finally forwards the RREP packet to previous node. To prevent resending the same RREP packet X will save it in its route reply buffer and if X receives it again from its neighbors then X will discard it. At the same time X will monitor its successor node and verifies that this node forwarded the RREP packet by using the control packet dropping prevention scheme.

8- If X doesn't find any existing entry in its routing table for pair <S, D> then it will create a new entry for pair<S, D> in its routing table with next hop equal to Y. Then X will sign RREP with timestamp and forwards it to previous node. At the same time X will monitor its successor node and verifies that this node forwards the RREP packet by using the control packet dropping prevention scheme.

9- Finally when S receives the RREP packet it first verifies the signature to authenticate the sender and validation of the RREP packet, if it correct then it will add a new entry for the destination node in its routing table and sends the data message from the queue to the next hop.

3.2.3 Path Maintenance Process

It may be summarized as follows. When any node along an established path moves, so that some of the nodes become unreachable, a RERR packet is wholly signed

with timestamp and sent to affected source node. Upon receiving a RERR packet the node first verifies the signature to authenticate the sender and validation of the RERR packet, if it correct then the node will check RERR packet for tunneling or wormhole attack by using temporal leash concept, if the RERR isn't tunneled then the node will delete the affected routing entries from its routing table and forwards the REER packet to the precursor node in the path. At the same time each node will monitor its successor node and verifies that this node forwarded the RERR packet by using the control packet dropping prevention scheme. This scheme will monitor, detect and isolate the suspicious node by adding it to its *Suspicious_List*. Finally when the source node S receives the REER packet it first verifies the signature to authenticate the sender and validation of the RERR packet, if it correct then S will check RERR packet for tunneling or wormhole attack by using temporal leash concept, if the RERR isn't tunneled then S will delete the affected routing entries from its routing table and restarts the path discovery process, if S still needs that route.

3.3 The difference between SWBAODV and WBAODV

WBAODV is unsecured routing protocol in MANET which considers the path stability problem and assumes all the nodes in the network are friendly. WBAODV enhances the performance, but this isn't enough because when there are suspicious nodes in the network launch many types of routing attacks then the improvement of the performance which WBAODV is done becomes useless.

On the other hand SWBAODV considers both of the path stability and security problems simultaneously. SWBAODV selects the stable path with maximum weight among all other possible feasible paths as the main routing path and also combines many effective security mechanisms together which can monitor, detect, isolate the suspicious nodes and prevent routing attacks.

Chapter 4

SWBAODV Security Analysis

In this chapter we will analyze our new proposed secure routing protocol against many famous and identified routing attacks in MANET to ensure its immunity against these attacks and how the combined security mechanisms and solutions which described in chapters 2 and 3 are cooperated together to make these attacks to fail.

4.1 MANET Security

Information Security (InfoSec) is defined as the practice of protecting information from accidental or intentional misuse by persons inside or outside of a system or organization. Although, an information security problem has a holistic approach in its solving mechanism, technical aspects of the problem have significant functionalities in this context. Confidentiality, integrity, availability, authorization and non-repudiation are the basic security requirements, which are considered in analyzing an information security problem.

Mobile ad hoc networks routing protocols are being designed without security in mind. In most of their specifications it is assumed that all the nodes in the network are friendly. The security issue has been postponed and there used to be the common feeling that it would be possible to make those routing protocols secure by retrofitting pre-existing cryptosystems. Nevertheless, securing network transmissions without securing the routing protocols is not sufficient. Moreover, by retrofitting cryptosystems, security is not necessarily achieved. Therefore, in MANET networks with security needs, there must be two security systems: one to protect the data transmission and one to make the routing protocol secure. There are already well studied point to point

security systems that can be used for protecting network transmissions. But there is not much work about how make MANET routing protocols discover routes in a secure manner.

The security schemes for the ad hoc networks routing protocols can be categorized into two approaches. The first one is the secure routing approach that aims to design and implement routing protocols with security features. While the second approach is the Intrusion Detection approach that aims to design and implement intrusion detection component in the ad hoc network

The security requirements for MANET routing protocols include:

(1) Source authentication: The receiver should be able to confirm that the identity of the source is indeed who or what it claims to be.

(2) Neighbor authentication: The receiver should be able to confirm that the identity of the sender (i.e., one hop previous node) is indeed who or what it claims to be.

(3) Message integrity: The receiver should be able to verify that the content of a message has not been altered either maliciously or accidentally in transit.

(4) Access control: It is necessary to ensure that mobile nodes seeking to gain access to the network have the appropriate access rights.

A node is malicious if it is an attacker that cannot authenticate itself as a legitimate node due to the lack of valid cryptographic information. A node is compromised if it is an inside attacker who is behaving maliciously but can be authenticated by the network as a legitimate node and is being trusted by other nodes. A node is selfish when it tends to deny providing services for the benefit of other nodes in order to save its own resources.

4.2 MANET Routing Attacks

In ad hoc networks, attacks can be classified into active and passive attacks. In passive attacks, attackers don't disrupt the operation of routing protocol but only attempt to discover valuable information by listening to the routing traffic. An active attacker injects packets into the network, eavesdrops and also tries to compromise the network with denial of service. In the active attacks, the malicious nodes introduce false information to confuse the network topology. They can either attract traffic to them and then drop or compromise the packets. They can also send false information and lead packets to the wrong node and cause congestion in one area. The attacks can either target at the routing procedure or try to flood the networks.

Most common attack patterns identified in ad hoc network environment are the following.

4.2.1 Modification Attack

Malicious nodes can modify the protocol fields of messages passed among nodes. Such attacks compromise the integrity of routing computation. By altering routing information, an attacker can cause network traffic to be dropped, redirected to a different destination or take a long route to the destination increasing communication delays. For example in figure (4.1) suppose that M is a malicious node and S wishes to communicate with X and that S has an unexpired route to X in its route cache. S transmits a data packet toward X with the source route S --> A --> B --> M --> C --> D --> X contained in the packet's header. When M receives the packet, it can alter the source route in the packet's header, such as deleting D from the source route. Consequently, when C receives the altered packet, it attempts to forward the packet to X. Since X cannot hear C, the transmission is unsuccessful.

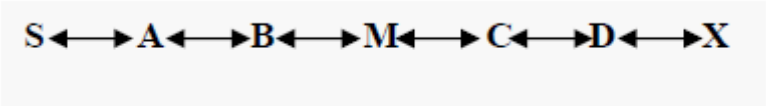

Figure (4.1): Example of modification attack in MANET

4.2.2 Fabrication Attack

Fabrication refers to attacks performed by generating false routing messages. Following is an example of an attack launched by sending false route error message. Suppose S has a route to D via nodes A and B, as in figure (4.2). A malicious node M can launch a denial-of-service attack by continually sending route error messages to A spoofing B, indicating a broken link between B and D. A receives the spoofed route error message thinking that it came from B. A deletes its routing table entry for D and forwards the route error message on to the upstream node, who then also delete its routing table entry. If M listens and broadcasts spoofed route error messages whenever a route is established from S to D, M can successfully prevent communications between S and D.

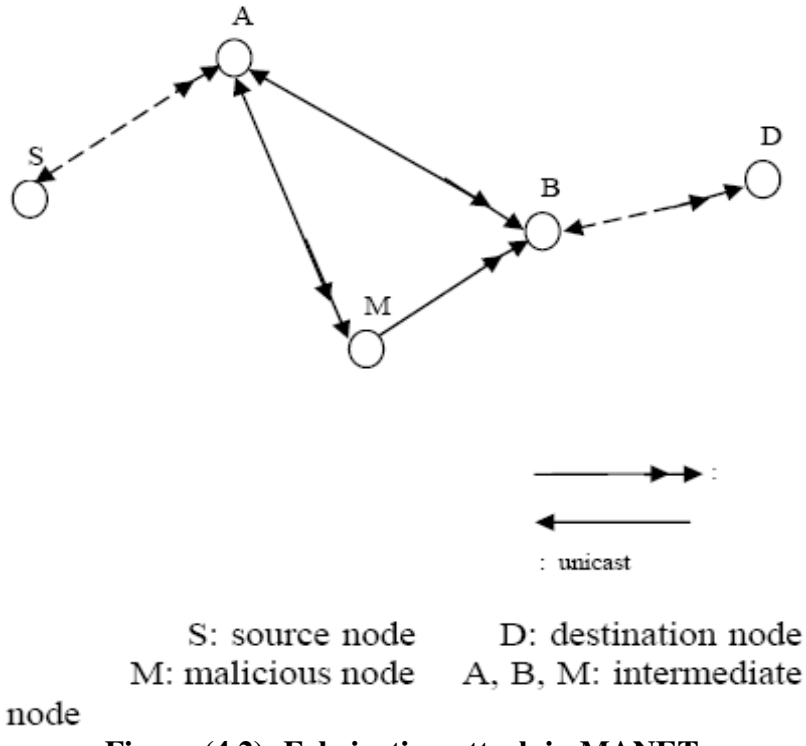

Figure (4.2): Fabrication attack in MANET

4.2.3 Spoofing Attack

A single malicious node in the ad hoc network can spoof the nodes identity in order to forward packets through it. Later the information can be used to create denial-of-service attacks.

4.2.4 Reply Attack

As topology changes, old control messages, though valid in the past, describe a topology configuration that no longer exists. An attacker can perform a reply attack by recording old valid control messages and re-sending them, to make other nodes update their routing tables with stale routes.

4.2.5 Rushing Attack

An offensive that can be carried out against on-demand routing protocols. Typically, on-demand routing protocols state that nodes must forward only the first received Route Request from each route discovery; all further received Route requests are ignored. This is done in order to reduce cluttering. The attack consists, for the adversary, in quickly forwarding its Route Request messages when a route discovery is initiated. If the Route Requests that first reach the target's neighbors are those of the attacker, then any discovered route includes the attacker.

4.2.6 Denial-of-Service (DoS) Attack

A denial of service attack in general could be launched at any layer of an ad hoc network. On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could break down high-level services. In the routing mechanism a source node sends route request messages to all neighbors to find a route

to the destination node. In the denial-of-service case a malicious node in between can successful send an erroneous route message to the source route to disrupt the service. For example a malicious node can redirect the network traffic and conduct DoS attacks by modifying message fields or by forwarding routing message with false values. In figure (4.3), M is a malicious node which can keep traffic from reaching X by continuously advertising to B a shorter route to X than the route to X that C advertises. In this way, malicious nodes can easily cause traffic subversion and denial of service (DoS) by simply altering protocol fields.

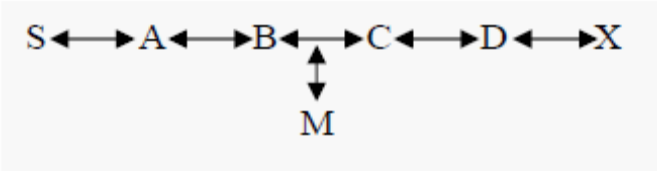

Figure (4.3): Example of DoS attack in MANET

4.2.7 Selfish Attack

By dropping RREQ (Route Request) or RREP (route reply) packets a selfish node could exclude itself from routes and thereby avoid receiving data packets to forward in order to save its power. Selfishness misbehavior can cause DoS later.

4.2.8 Routing Tables Overflow Attack

Routing tables overflow attack attempts to create routes to nonexistent nodes. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. The proactive algorithms are more vulnerable to table overflow attacks than reactive algorithms because they attempt to discover routing information with time intervals.

4.2.9 Sybil Attack

The Sybil attack refers to represent multiple identities for malicious intent. This can be achieved if the malicious nodes collude and share their secret keys. As illustrated in figure (4.4), A is connected with B, C and the malicious node, M1. If M1 represents other nodes M2, M3 and M4 (e.g. by using their secret keys), this makes A believe it has 6 neighbors instead of 3. In a mobile ad hoc network that uses multi-path routing, the possibility of choosing a path that contains a malicious node (e.g. M1) will be largely increased.

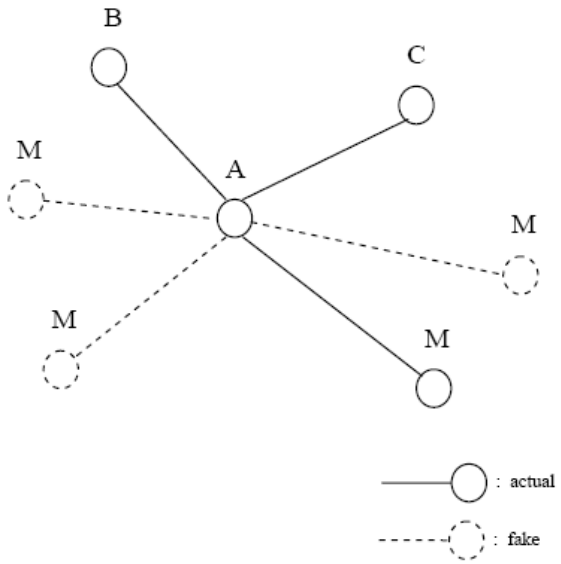

Figure (4.4): Sybil attack in MANET

4.2.10 Blackhole Attack

In Black hole attack a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. In second step, the attacker consumes the packets and never forwards. In an advanced form, the attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected. In this way, the attacker falsified the neighboring nodes that monitor the ongoing packets. In figure (4.5), node 1 wants to send data packets to node 4 and initiates the route discovery process. We assume that node 3 is a

malicious node and it claims that it has route to the destination whenever it receives RREQ packets, and immediately sends the response to node 1. If the response from the node 3 reaches first to node 1 then node 1 thinks that the route discovery is complete, ignores all other reply messages and begins to send data packets to node 3. As a result, all packets through the malicious node is consumed or lost.

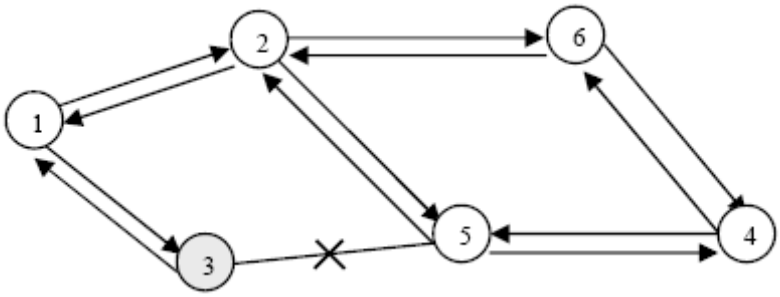

Figure (4.5): Blackhole Attack in MANET

4.2.11 Tunneling Attack

Ad hoc networks have an implicit assumption that any node can be located adjacent to any other node. A tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. One vulnerability is that two such nodes may collaborate to falsely represent the length of available paths by encapsulating and tunneling the routing message between them. In figure (4.6), M1 and M2 are two malicious nodes that encapsulate data packets and falsified the route lengths. Suppose node S wishes to form a route to D and initiates route discovery. When M1 receives a RREQ from S, M1 encapsulates the RREQ and tunnels it to M2 through an existing data route, in this case {M1 --> A --> B --> C --> M2}. When M2 receives the encapsulated RREQ on to D as if had only traveled {S --> M1 --> M2 --> D}. Neither M1 nor M2 update the packet header. After route discovery, the destination finds two routes from S of unequal length: one is of 5 and another is of 4. If M2 tunnels the RREP back to M1, S would falsely consider the path to D via M1 is

better than the path to D via A. Thus, tunneling can prevent honest intermediate nodes from correctly incrementing the metric used to measure path lengths.

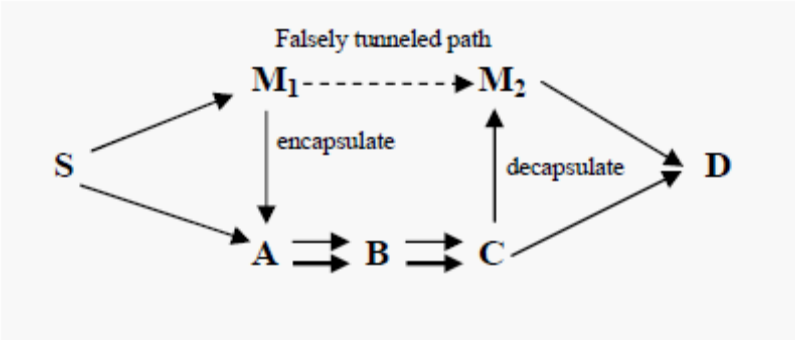

Figure (4.6): Path length spoofed by Tunneling

4.2.12 Wormhole Attack

In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. It is called tunneling attack because the colluding malicious nodes are linked through a private network connection which is invisible at higher layers. In figure (4.7) two attackers M1 and M2, connected by a high-speed off-channel link, are strategically placed at different ends of a network. These attackers then record the wireless data they overhear, forward it to each other, and replay the packets at the other end of the network. Replaying valid network messages at improper places, wormhole attackers can make far apart nodes believe they are immediate neighbors, and force all communications between affected nodes to go through them.

.

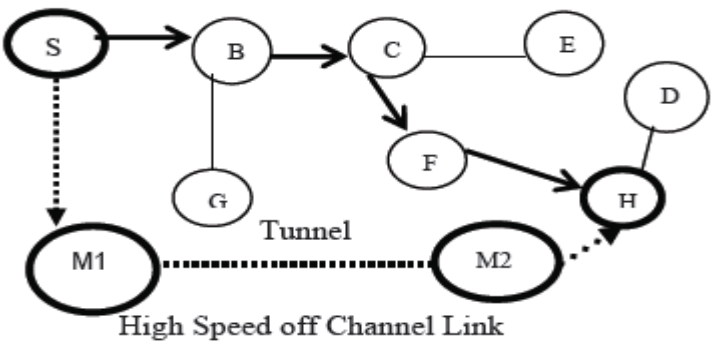

Figure (4.7): Wormhole Attack in MANET

4.2.13 Flooding Attack

In the Ad Hoc Flooding Attack, the attack node violates the rules to exhaust the network resource. Firstly, the attacker selects many IP addresses which are not in the networks if he knows the scope of IP address in the networks. Because no node can answer RREP packets for these RREQ, the reverse route in the route table of node will be conserved for longer. The attacker can select random IP addresses if he can not know scope of IP address. Secondly, the attacker successively originates mass RREQ messages for these void IP addresses. The attacker tries to send excessive RREQ without considering RREQ_RATELIMIT within per second. The attacker will resend the RREQ packets without waiting for the RREP or round-trip time, if he uses out these IP addresses. The TTL of RREQ is set up to a maximum without using expanding ring search method. In the Flooding Attacks, the whole network will be full of RREQ packets which the attacker sends. The communication bandwidth is exhausted by the flooded RREQ packets and the resource of nodes is exhausted at the same time. Figure (4.8) shows an example of the flooding attack where node H is the attacker and try to flood the network.

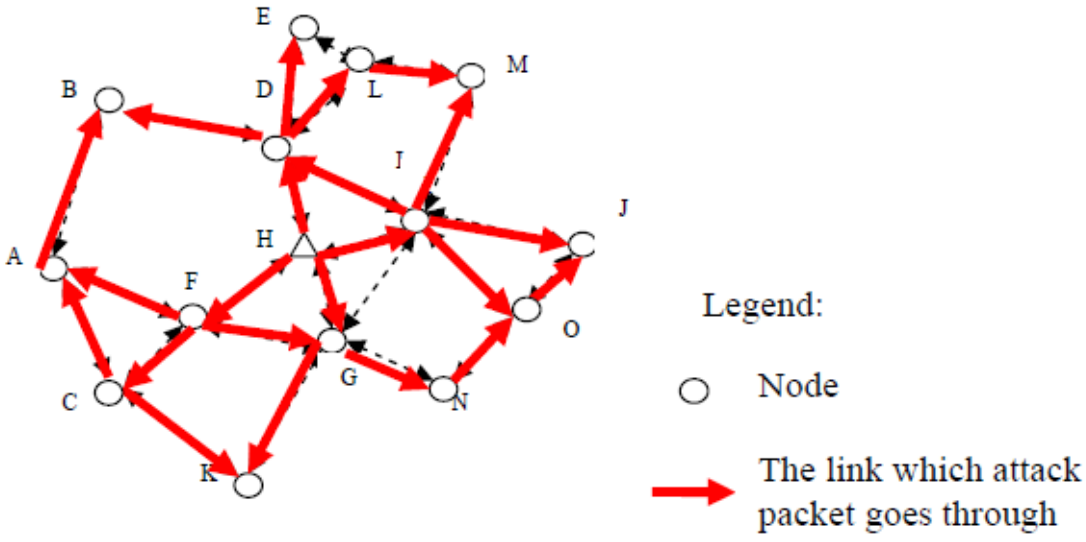

Figure (4.8): Flooding Attack in MANET

4.3 Evaluation of Secure Routing Protocols against Attacks

In this section we analyzed six of famous secure routing protocols in MANET against the most commonly routing attacks which are described in the previous section.

4.3.1 SEAD

SEAD was developed based on Destination Sequenced Distance Vector (DSDV) protocol and incorporates One-Way Hash function to authenticate in the routing update mechanism in order to enhance the routing security. Securing a table driven protocol is harder than securing an on demand protocol due to the existence of predefined routes. Distance vector protocols encapsulate the route information into a hop count value and a next hop. An attacker cannot create a valid route with a larger sequence number that it received due to the properties of hash function. As SEAD incorporates neighbor authentication through Hash functions, an attacker can not compromise any node. SEAD is prone through wormhole attack. Even if authentication is provided using hash functions, a wormhole attack is possible through tunneling the packets from one location and retransmitting them from other location into the network. All packets in the wormhole attack flow in a circle around instead of reaching the destination. Routing table overflow attacks are possible in SEAD, as SEAD is developed based on a table driven approach. A compromised node can advertise routes to nodes which are not in the network and there by fill in the space allocated in the routing table with false node routes. Spoofing attack is possible through compromised node acting like a destination node in the route discovery process by spoofing the identity of the destination node that can cause route destruction. Blackhole attack is also possible through a compromised node advertising the shortest roots to non-existing nodes in the network. Tunneling and DOS attacks are also possible through compromised nodes. Table driven protocols are much more prone to security threats. Rushing, Sybil, Selfish and Flooding attacks are

possible because there are no any existing security mechanisms to cope these attacks in SEAD routing protocol.

4.3.2 Ariadne

Ariadne was developed based on an on demand protocol, Dynamic Source Routing (DSR). Ariadne uses MAC s and shared keys between nodes to authenticate between nodes and use time stamps for packet lifetime. Wormhole attacks are possible in Ariadne through two compromised nodes. Ariadne prevents spoofing attacks with time stamps. The use of source routes prevents loops, since a packet passing through only legitimate nodes will not be forwarded into a loop due to time stamps. Rushing, Sybil, Selfish and Flooding attacks are possible because there are no any existing security mechanisms to cope these attacks in Ariadne routing protocol.

4.3.3 SRP

Secure routing protocol (SRP) was developed based on Dynamic Source Routing (DSR). The intermediate nodes participating in the route discovery measure the frequency of queries received from their neighbors and maintains a priority ranking inversely proportional to the query rate. So the malicious compromised nodes participating in the network are given least priority to deal with. The security analysis of SRP is similar to Ariadne as both are based on DSR protocol.

4.3.4 ARAN

ARAN uses public key cryptography and a central certification authority server for node authentication and neighbor node authentication in route discovery. Denial-of-service attacks are possible with compromised nodes. Malicious nodes cannot initiate an attack due to the neighbor node authentication through certificates. Participating nodes broadcast unnecessary route requests across the network. An attacker can cause

congestion in the network, there by compromising the functionality of the network. Spoofing attacks are prevented by ARAN through node level signatures. Each packet in the network is signed by its private key before broadcasted to the next level and checked for the authentication. So spoofing the identity of node is hampered by ARAN. Due to the strong cryptographic features of ARAN, malicious nodes cannot participate in any type of attack patterns. Only compromised nodes can participate in any attack pattern. Tunneling attacks are possible in ARAN. Two compromised neighbor nodes can collaborate to falsely represent the length of available paths by encapsulating and tunneling the routing message between them. Wormhole attack is also possible through two compromised nodes. Table overflow, blackhole attacks are impossible due to node level authentication with signatures. Rushing, Sybil, Selfish and Flooding attacks are possible because there are no any existing security mechanisms to cope these attacks in ARAN routing protocol.

4.3.5 SAODV

SAODV is a widely implemented protocol in industry due to its strong security features. SADOV uses a central key management in its routing topology. Digital signatures are used to authenticate at node level and hash chain is used to prevent the altering of node counts. Tunneling attacks are possible through two compromised nodes. Wormhole attacks are always possible with compromised nodes in any ad hoc network topology. The use of sequence numbers could prevent most of the possible reply attacks. Rushing, Sybil, Selfish and Flooding attacks are possible because there are no any existing security mechanisms to cope these attacks in SAODV routing protocol.

4.3.6 SAR

SAR was developed using a trust-based framework. Each node in the network is assigned with a trust level. So the attacks on this framework can be analyzed based on trust level and message integrity. Trust Level: SAR routing mechanism is based on the behavior associated with the trust level of a user. It is a binding between the identity of the user and the associated trust level. To follow the trust-based hierarchy, cryptographic techniques like: encryption, public key certificates, shared secrets, etc. are employed. Message integrity: The compromised nodes can utilize the information flow in between nodes and reading of packets to launch attacks. It results in corruption of information, confidentiality of the information, and in denial of network services. The Security analysis on the attack patterns is based on the trust based framework. So the analysis depends on the key management used and the cryptographic systems applied. In general the security analysis of SAR is similar to SAODV routing protocol.

4.4 Evaluation of SWBAODV against Attacks

In this section we analyzed our new secure routing protocol against the most commonly routing attacks which are described in the section 4.2.

4.4.1 Modification Attack

SWBAODV uses security primitives like hash chains to secure mutable message field (hop count) and digital signature to secure the non-mutable fields. Any malicious node try to modify the content of the routing message, then the next hop node will discover the modification and will discard the message because we can’t get two different messages have the same signature. So SWBAODV is secure against modification attack.

4.4.2 Fabrication Attack

SWBAODV uses digital signature to authenticate the RERR messages and the non-mutable fields of the RREQ and RREP messages. It is also provides an end-to-end authentication and node-to-node verification of these messages. So SWBAODV is secure against fabrication attack.

4.4.3 Spoofing Attack

SWBAODV uses digital signature to authenticate the identity of the nodes and to provide an end-to-end authentication and node-to-node verification of the routing messages. So SWBAODV is secure against spoofing attack.

4.4.4 Reply Attack

SWBAODV uses digital signature with timestamp to cope this attack. When a node receives a message it verifies the signature to authenticate the sender and then checks the timestamp to validate the message's freshness. When a node finds that the received message is old then it will discard it. Also another thing we can use as a pointer of the freshness of the routing messages is the Sequence Number of the message which is a non-mutable field and is increased monotonically when a node initiates new routing messages. So SWBAODV is secure against reply attack.

4.4.5 Rushing Attack

SWBAODV uses digital signature to authenticate the sender's identity, then on contrary of on-demand routing protocols, SWBAODV depends on the stable weight-based routing strategy that allows node to forward all the RREQ packets that received and which have larger weight than it has in its reverse route entry table for that source-destination pair. Then destination node selects the stable path with maximum weight among all feasible paths as a main routing path. This process doesn't guarantee that the

attacker be in the main routing path. The basis of the attack is overcome because the probability of the attacker to falsely be in the routing path is very low. So SWBAODV is secure against rushing attack.

4.4.6 Denial-of-Service Attack

SWBAODV uses control packets dropping prevention scheme to cope this attack. This scheme will monitor, detect and isolate the suspicious nodes. So SWBAODV is secure against DoS attack There are two main metrics that we can used to evaluate the efficiency of control packets dropping prevention scheme: true isolation rate and false isolation rate. True Isolation Rate (TIR) or true positives, represents the efficiency on packet droppers isolation. It is the average rate of true isolation computed as follows:

$$TIR = \sum_{i=1, m_i \neq 0}^{n} \frac{ti_i / m_i}{k}$$

Where ti_i: is the true isolation of node i, i.e. the number of misbehaving nodes monitored and detected by node i, then isolated in the network. m_i: the number of misbehaving nodes monitored by node i. n: the number of nodes. k: the number of nodes that have monitored misbehaving nodes (whose $m_i \neq 0$). False Isolation Rate (FIR) is very similar to the previous one. It is the average rate of false isolations, given by the following formula:

$$FIR = \sum_{i=1, m'_i \neq 0}^{n} \frac{fi_i / m'_i}{k'}$$

Where fi_i is the false isolations of node i, i.e. the number of well-behaved nodes monitored and wrongly detected by node i and isolated, m'_i is the number of well-behaving nodes monitored by node i, and finally k' is number of nodes that have monitored well-behaving nodes (whose $m'_i \neq 0$).

We evaluated the efficiency of control packets dropping prevention scheme which prevent the DoS attack by using simulations with 50 nodes. These simulations are based on the model and parameters which are described in section 5.2 and table 5.1.

Figures (4.9) and (4.10) show the true isolation rate and false isolation rate of SWBAODV routing protocol with different node's mobility speeds, respectively. These results were obtained by simulating RERR dropping (malicious behavior) which allow the malicious nodes to launch the denial-of-service attack by preventing the destruction of broken routes.

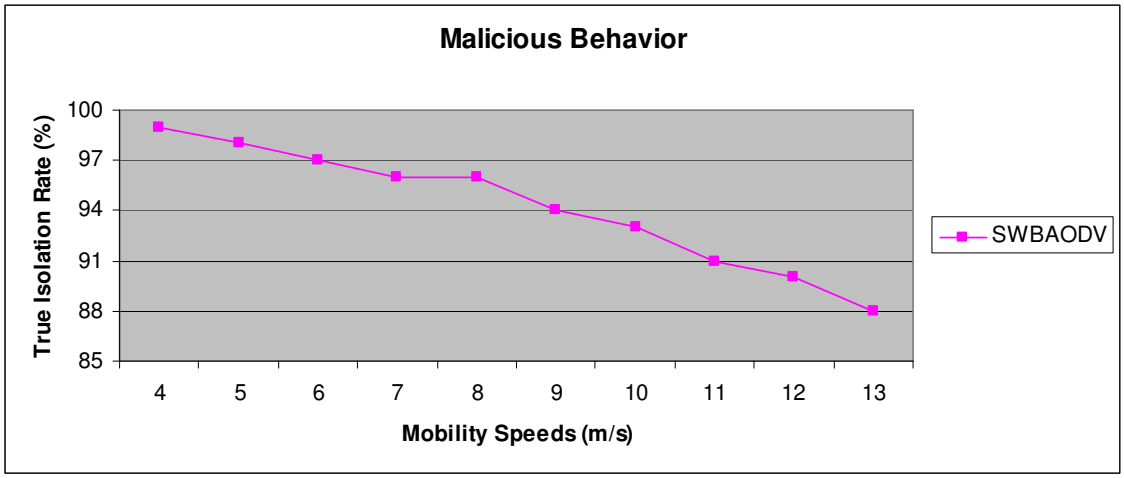

Figure (4.9): True Isolation Rate versus mobility speeds with 50 nodes

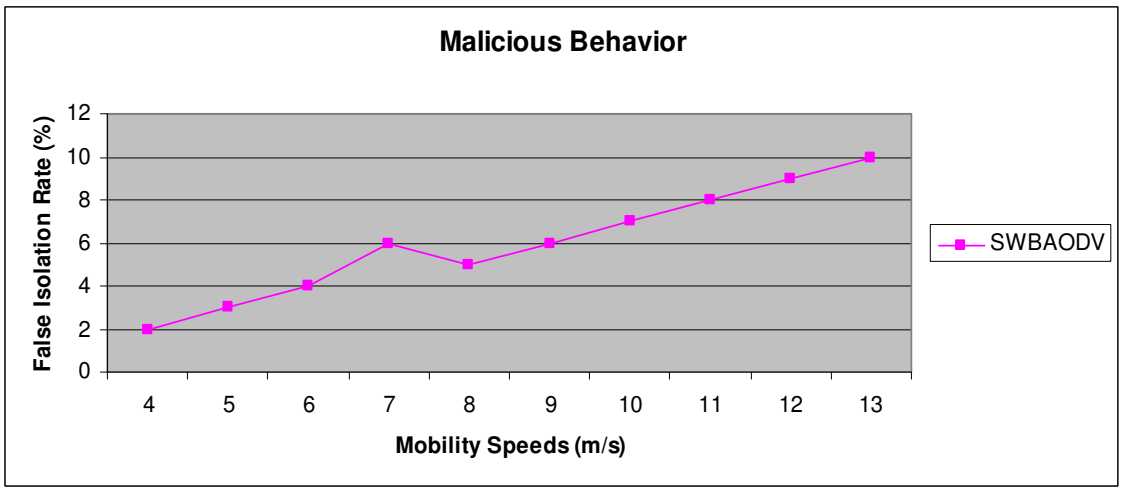

Figure (4.10): False Isolation Rate versus mobility speeds with 50 nodes

We can observe that SWBAODV clearly outperforms all six secure routing protocols which are described in section 4.3 with respect to packet dropper isolation, since those latter simply do not detect such a misbehavior. Figure (4.9) shows how SWBAODV, has high true isolations, especially in high mobility environment. We can also observe that the true isolation rate is decreased when the mobility speed is increased and that due to the increased probability of packet dropping which happened due to the route failures rather than malicious drops, but SWBAODV may falsely detected it as malicious behavior. Although of the decreasing in the true isolation rate when the mobility speed is increased the results are still very high and the true isolation rate equals to 88% when the mobility speed equals to 13 m/s. On the other hand, figure (4.10) shows that the false isolation rate is very low and it didn't exceed 10 % when the mobility speed equals to 13 m/s. It is more importantly that the SWBAODV is less affected with the mobility in comparison of other secure routing protocols in MANET.

4.4.7 Selfish Attack

SWBAODV uses control packets dropping prevention scheme to cope this attack. This scheme will monitor, detect and isolate the suspicious nodes. So SWBAODV is secure against selfish attack. We evaluated the efficiency of control packets dropping prevention scheme against the selfish attack in the same way that we are used in the previous sub section by using simulations with 50 nodes. These simulations are based on the model and parameters which are described in section 5.2 and table 5.1.

Figures (4.11) and (4.12) show true isolation rate and false isolation rate of SWBAODV routing protocol with different node's mobility speeds, respectively. These results were obtained by simulating RREQ and RREP dropping (selfish behavior) which allow the selfish nodes to prevent themselves from being included in routes.

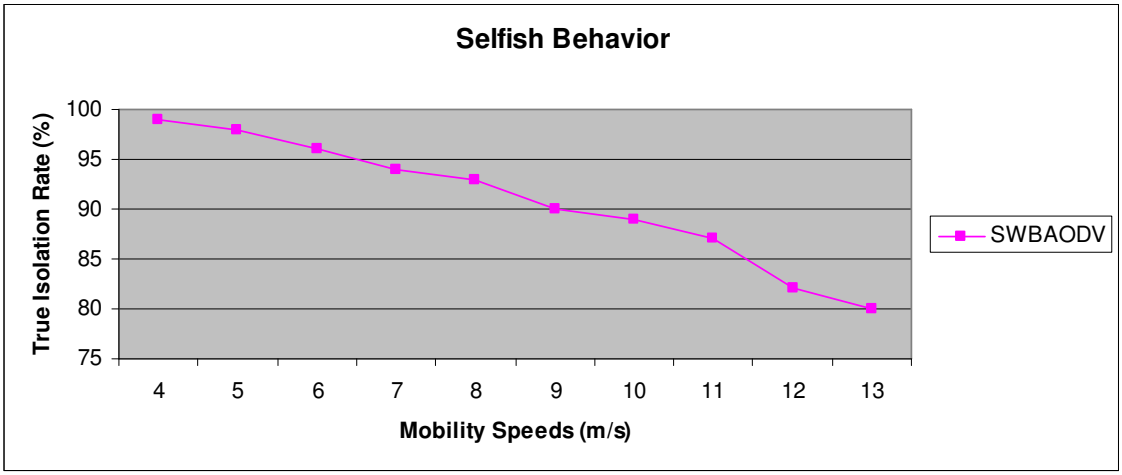

Figure (4.11): True Isolation Rate versus mobility speeds with 50 nodes

We can observe that SWBAODV clearly outperforms all six secure routing protocols which are described in section 4.3 with respect to packet dropper isolation, since those latter simply do not detect such a misbehavior. Figure (4.11) shows how SWBAODV has high true isolations, especially in high mobility environment. We can also observe that the true isolation rate is decreased when the mobility speed is increased and that due to the increased probability of packet dropping which happened due to the route failures rather than malicious drops, but SWBAODV may falsely detected it as selfish behavior. Although of the decreasing in the true isolation rate when the mobility speed is increased the results are still very high and the true isolation rate equals to 80% when the mobility speed equals to 13 m/s. On the other hand, figure (4.12) shows that the false isolation rate is very low and it didn't exceed 15 % when the mobility speed equals to 13 m/s. This increase of false isolation rate in figure (4.12) in comparison of that in figure (4.10) is due to that the number of RREQ and RREP messages is more than the number of RERR messages. It is more importantly to note that the SWBAODV is less affected with the mobility in comparison of other secure routing protocols in MANET.

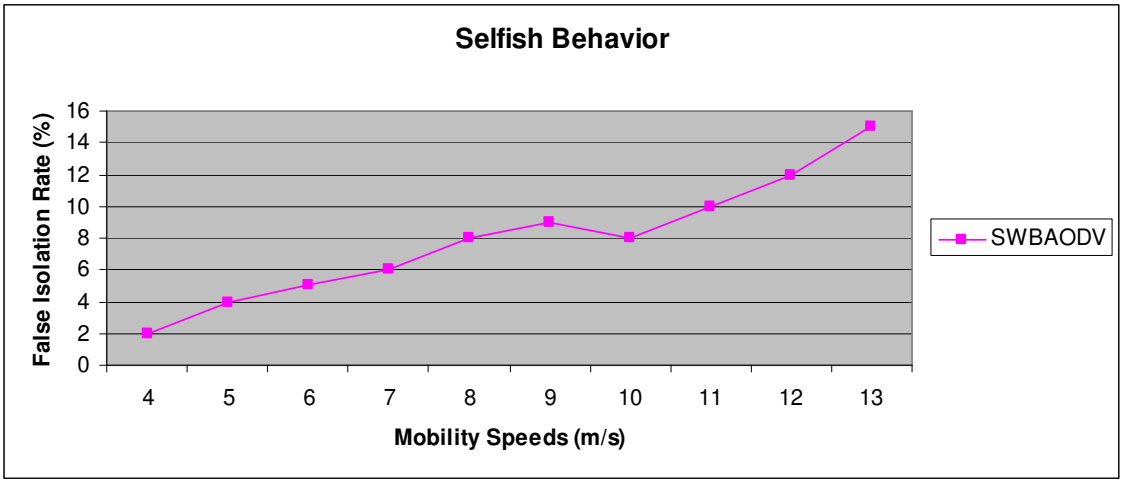

Figure (4.12): False Isolation Rate versus mobility speeds with 50 nodes

4.4.8 Routing Tables Overflow Attack

SWBAODV is on-demand routing protocol and uses digital signature to authenticate the identity of the nodes, provide an end-to-end authentication and node-to-node verification of the routing messages. Also the destination is only allowed to reply to RREQ packets. So SWBAODV is secure against routing table overflow attack.

4.4.9 Sybil Attack

SWBAODV uses digital signature to authenticate the identity of the nodes, provide an end-to-end authentication and node-to-node verification of the routing messages. Also the destination node is only allowed to reply to RREQ packets and selects the stable path with the maximum weight among all feasible paths depending on weight-based routing strategy. This process doesn't guarantee that the attacker be in the main routing path. So SWBAODV is secure against Sybil attack.

4.4.10 Blackhole Attack

SWBAODV strict that only the destination node can reply to RREQ packets, so the basis of the attack is overcome. When a malicious node receives a RREQ packet and it isn't the destination node then SWBAODV forces this node to forward the packet to

its neighbors even if it knows the fresh route to the destination because SWBAODV uses the stable weight-based routing strategy which selects the routing path with the maximum weight and it isn't necessary the shortest path as in other on-demand routing protocols. Also if we suppose that the malicious node is located in the routing path between the source and the destination nodes and try to drop packets, then packet dropping prevention scheme will monitor, detect and isolate the suspicious node. So SWBAODV is secure against blackhole attack.

4.4.11 Tunneling Attack

SWBAODV uses temporal leash concept to cope this attack. When any node receives any routing message first it verifies the sender, then it will check the expiration time of the packet to detect if the packet traveled further than the leash allows and discards it if that happened. So SWBAODV is secure against tunneling attack.

4.4.12 Wormhole Attack

SWBAODV uses temporal leash concept to allow the receiver of a packet to detect if the packet traveled further than the leash allows and discards it if that happened. So SWBAODV is secure against wormhole attack. We evaluated the efficiency of temporal leash concept to prevent the wormhole attack by using simulations with 50 nodes. These simulations are based on the model and parameters which are described in section 5.2 and table 5.1.

Figure (4.13) shows the wormhole link detection rate as a function of the tunnel length. Tunnel length refers to the number of hops between the malicious nodes. We define a wormhole link detection rate as the proportion of the number of detected links that contain wormhole tunnel to all links that contain wormhole tunnels. The results show that a wormhole is more detected in the configuration where this attack is launched on a longer hops count. This result is quite obvious, since through a wormhole

tunnel, packets are encapsulated and decapsulated repeatedly, which leads to a more delayed transmissions. In the case of less than 3 hops, detection rate is relatively low, but this isn't important because in real MANET the tunnel length is more than 4 hops.

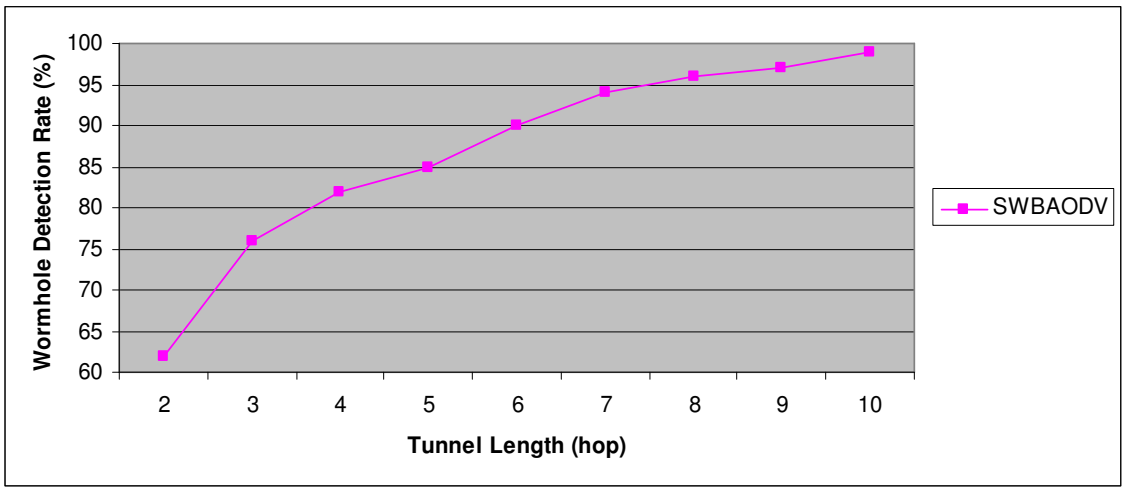

Figure (4.13): Wormhole Link Detection Rate versus Tunnel Length with 50 nodes

Figure (4.14) shows the results of the wormhole detection accuracy. Detection accuracy is measured as the ratio of links that contain effectively wormhole tunnels to the links that are judged suspicious by temporal leash concept. The results show that the detection accuracy depends on the tunnel length. However, the detection accuracy increased dramatically as the tunnel length increased. But we can observe that the wormhole detection accuracy decreased when the mobility speed increased more than 7 m/s and this can be explained by the number of neighbors that can be selected to form wormhole tunnels by malicious nodes. However, if the number of nodes in the network becomes larger, the malicious nodes are more likely to have many neighbors even though they are far away from each others and connected through a longer wormhole tunnel. Moreover, each node sends periodically routing control messages, which increases the load in dense networks. As these routing control messages are tunneled through the wormhole tunnel, the traffic increases dramatically and congestion becomes inevitable through the path of that wormhole tunnel. This makes the legitimate nodes

suspect and decide faultily some links as containing wormhole tunnels because of the increased delays. Although of this decreasing in the detection accuracy the results are still very high and the wormhole detection accuracy equals to 85% when the mobility speed equals to 13 m/s.

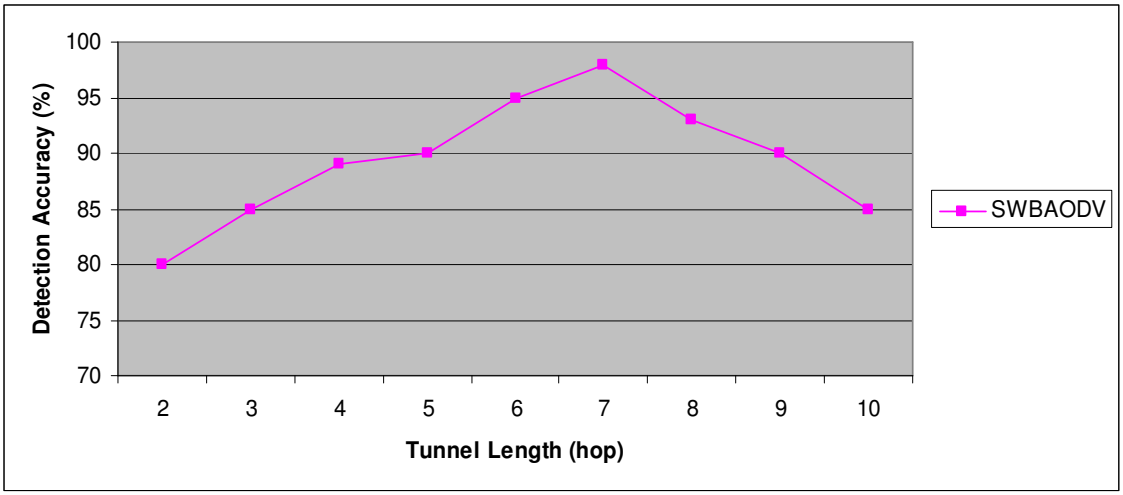

Figure (4.14): Wormhole Detection Accuracy versus Tunnel Length with 50 nodes

4.4.13 Flooding Attack

SWBAODV uses the flooding attack prevention scheme to cope this attack. This scheme will detect and isolate the attacker. So SWBAODV is secure against flooding attack. We evaluated the efficiency of flooding attack prevention scheme by using simulations with 50 nodes. These simulations are based on the model and parameters which are described in section 5.2 and table 5.1. In order to carefully observe the impact on performance of mobile ad hoc networks, we assumed that rates of attacking packets are respectively, 30 packets/second and 50 packets/second. In other words, the intruder respectively floods 30 and 50 packets every second. We calculated packet delivery rate every 100 seconds. At 100 seconds of simulation experiment, we totalized packet delivery rate from 0 to 100 seconds. At 200 seconds of simulation experiment, we totalized packet delivery rate from 100 to 200 seconds. The rest may be deduced by analogy. There is not attacking packets from 0 to 300 seconds in all scenarios. The

intruder starts to attack at 300 seconds to 900 seconds. The simulation results are as follows. Figures (4.15) and (4.16) show the performance of SWBAODV and WBAODV routing protocols under 30 and 50 attacking packets every second, respectively.

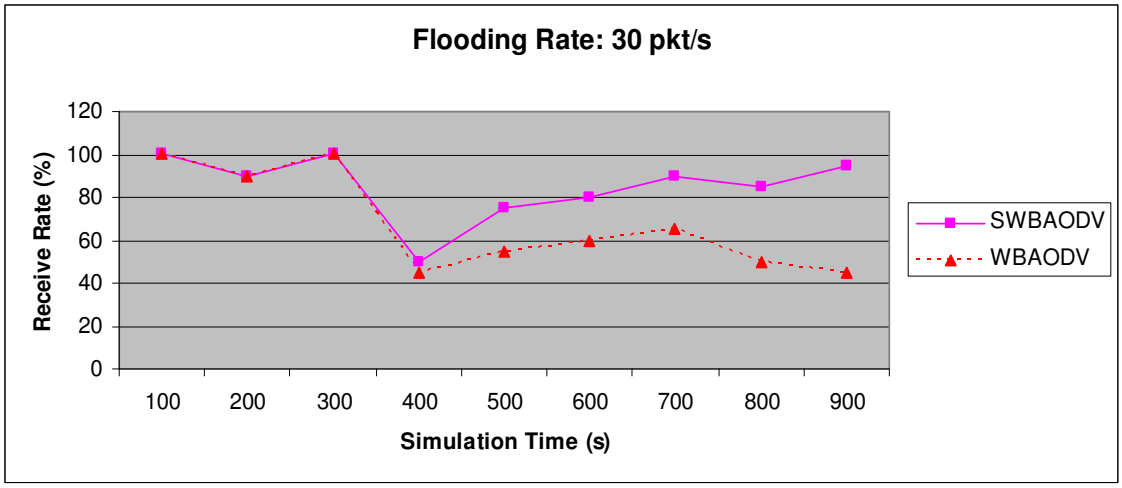

Figure (4.15): Receive Rate versus Simulation time under 30 attacking packets

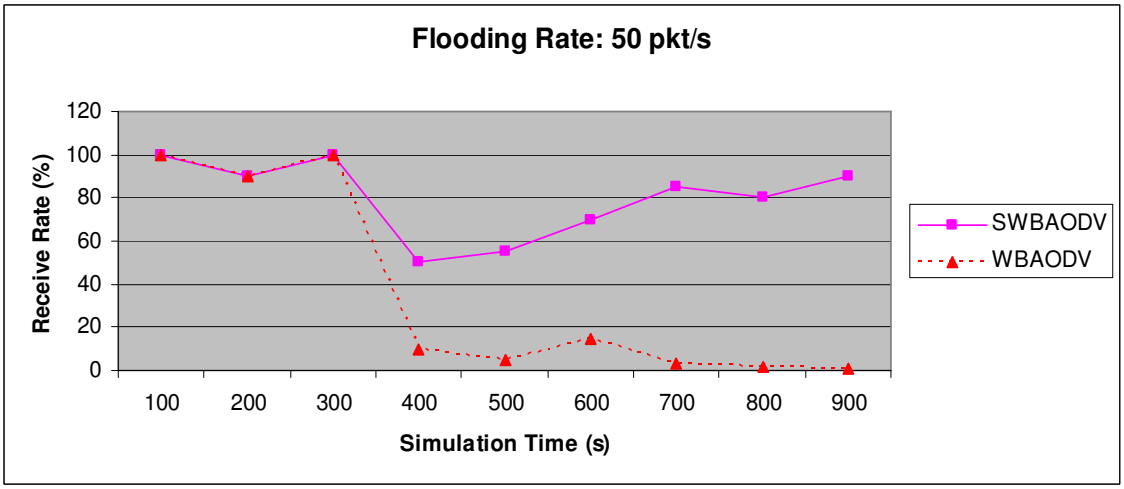

Figure (4.16): Receive Rate versus Simulation time under 50 attacking packets

We can observe that the performance of SWBAODV is better than that of WBAODV routing protocol, because SWBAODV is integrated with FAP. In figure (4.15) the packet delivery ratio of SWBAODV increased from 50% to 95% after the attack is started. In figure (4.16) with more attacking packets every second, the

performance of WBAODV network falls quickly. When FAP takes effect, the performance of SWBAODV becomes better and packet delivery rate keep up about 90%. It implies that the Flooding Attack Prevention scheme efficiently resists the Ad Hoc Flooding Attack by identifying the attackers and isolating them from the networks.

4.5 Comparison between SWBAODV and other Secure Routing Protocols

In this section we will compare between SWBAODV and six of secure routing protocols in MANET according to their immunity against routing attacks. From the results which we obtained in sections 4.3 and 4.4 we can make the comparison between them. The following Table (4.1) shows the mapping between the attack patterns and the secure routing protocols. Note that Y indicates that the attack is possible and the secure routing protocol is vulnerable against this attack also N indicates that the attack is not possible and the secure routing protocol is immune against this attack.

From this comparison we can see that SEAD is the weakest and the SWBAODV is the strongest. Also all the proposed secure routing protocols success to prevent some attacks and fail in others, But SWBAODV success to prevent or mitigate all of them because it use multiple security solutions and mechanisms that combined together with weight-based routing strategy which all cooperated well to build secure and robust routing protocol.

Table (4.1): Comparison between Secure Routing Protocols and SWBAODV

Attack Patterns	Ad hoc Secure Routing Protocols						
	SEAD	**Ariadne**	**SRP**	**ARAN**	**SAODV**	**SAR**	**SWBAODV**
Modification	N	N	N	N	N	N	N
Fabrication	Y	N	N	N	N	N	N
Spoofing	Y	N	N	N	N	N	N
Reply	Y	Y	Y	Y	Y	Y	N
Rushing	Y	Y	Y	Y	Y	Y	N
DoS	Y	Y	Y	Y	Y	Y	N
Selfish	Y	Y	Y	Y	Y	Y	N
Routing table overflow	Y	N	N	N	N	N	N
Sybil	Y	Y	Y	Y	Y	Y	N
Blackhole	Y	N	N	N	N	N	N
Tunneling	Y	Y	Y	Y	Y	Y	N
Wormhole	Y	Y	Y	Y	Y	Y	N
Flooding	Y	Y	Y	Y	Y	Y	N

Y = Attack possible, N = Attack not possible

4.6 SWBAODV and Security Goals

The ultimate goals of the security solutions for MANETs are to provide security services, such as authentication, confidentiality, integrity, authentication, non-repudiation, and availability to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack. The common security services are described below.

1- Availability: ensures the survivability of network services despite denial of service attack. SWBAODV provide availability when it prevents denial of service attacks.

2- Confidentiality: ensures that certain information is never disclosed to unauthorized entities. SWBAODV doesn't provide confidentiality directly, because in network layer the routing information is not secret. But SWBAODV can provide privacy by applying another layer of encryption/decryption above SWBAODV.

3- Integrity: guarantees that a message being transferred is never corrupted. SWBAODV provide message integrity, because it uses digital signature and hash chains to secure routing messages.

4- Authentication: enables a node to ensure the identity of the peer node it is communicating with. SWBAODV provide an end-to-end authentication and node-to-node verification of routing messages, because it uses the digital signature with timestamp.

5- Non-repudiation: ensures that the origin of a message cannot deny having sent the message. SWBAODV provide non-repudiation, because it uses the digital signature with timestamp.

Chapter 5

SWBAODV Performance Analysis

After we proposed our SWBAODV routing protocol and analyzed it against the most common attacks in MANET which prove its immunity against these attacks, now we will test its performance. To do that we will implement SWBAODV protocol and then we will subject it to extensive tests with many well-known ad hoc performance metrics. We choose the popular network simulator Java In Simulation Time for Scalable Wireless Ad hoc Networks (JiST/SWAN) as the simulator primarily to implement methods because it is widespread use in the academic community and the comprehensive manuals and tutorials that are freely available. It is possible to simulate a mobile multi-hop ad hoc wireless network in JiST/SWAN using simulated 802.11 MAC layer.

5.1 JisT/SWAN Simulator

We implement the SWBAODV routing protocol with JiST/SWAN simulation tool and we use this tool to ensure the new protocol efficiency. JiST/SWAN refers to Java in Simulation Time Scalable Wireless Ad hoc Network Simulator. JiST is a high-performance discrete event simulation engine that runs over a standard Java virtual machine. It is a prototype of a new general-purpose approach to building discrete event simulators, called virtual machine-based simulation that unifies the traditional systems and language-based simulator designs. The resulting simulation platform is surprisingly efficient. SWANS is a scalable wireless network simulator built atop the JiST platform. It was created primarily because existing network simulation tools are not sufficient for current research needs, and its performance serves as a validation of the virtual

machine-based approach to simulator construction. SWANS is organized as independent software components that can be composed to form complete wireless network or sensor network configurations. Its capabilities are similar to ns2 and GloMoSim, but is able to simulate much larger networks. SWANS leverages the JiST design to achieve high simulation throughput, save memory, and run standard Java network applications over simulated networks. In addition, SWANS implements a data structure, called hierarchical binning, for efficient computation of signal propagation [39].

The AODV code is a part of the SWAN code base. First we modify this code to accomplish standard WBAODV routing protocol which described in section 2.3. After we test WBAODV and ensure its performance we modify its code to accomplish our SWBAODV routing protocol which described in section 3.2.

5.2 Simulation Setup (model)

We decide to use a simulator for performance study because a practical implementation of an ad hoc network was obviously not feasible. As shown in table (5.1), we first made some assumptions on the parameters of the system architecture in the simulations.

Table (5.1): Parameters which are used in Simulations

Parameters	Value
Area	600x600 m^2
No. of nodes	40-120
Simulation duration	600 sec
No. of repetitions	6 times
Radio transmission range	100 m
Physical/MAC layer	IEEE 802
Pause time	100 sec
Mobility model	Random waypoint model
Node movement	4-13 m sec^{-1}
Data sending rate	2 Kbps
Each packet	2 MB

The simulations modeled a network in a 600 x 600 m^2 area with 40 to 120 mobile nodes. The radio transmission range for each node was assumed to be 100 meters. The speed of each mobile node was assumed varied from 4 to 13 m sec^{-1}. In these simulations we used the same communication pattern for all mobility simulations. The traffic pattern consisted of Constant Bit Rate (CBR) traffic type. In these simulations we did not use TCP because we did not want to investigate TCP, which uses flow control, retransmit features and so on. The communication traffic and scenarios simulations are randomly generated by JiST/SWAN itself. The initial positions of the nodes were uniformly distributed throughout the network. Node mobility was simulated according to the random waypoint mobility model, in which each node travels to a randomly selected location at a configured speed and then pauses for a configured pause time, before choosing another random location and repeating the same steps. Each simulation was run for 600 second.

Table (5.2) illustrates the best values of the parameters that are used with control packet dropping prevention scheme for both the directed and broadcast packets. Also table (5.3) illustrates the best values of the parameters that are used with flooding attack prevention scheme. In wormhole attack prevention scheme using temporal leash we assumed that the synchronization error can be as low as 183 ns with probability $1\text{-}10^{-10}$.

Table (5.2): Control Packets Dropping Prevention Scheme best parameters' values

Packet type	Parameters	Value
Directed packets	Tolerance threshold	3
	Number of witnesses	2
	Redemption pace	0.2
Broadcast packets	Tolerance threshold	1
	Number of witnesses	2
	Redemption pace	0.8

Table (5.3): Flooding Attack Prevention Scheme best parameters' values

Parameters	Value
Rate_RREQ_Threshold	10
Flooding_Intruder_Discovery_Interval	1 sec

5.3 Experimental Results

After we implemented SWBAODV routing protocol using JiST/SWAN simulator we tested its performance with some of MANET secure routing protocols. Due to code availability and time limitations we compared SWBAODV with only two of famous MANET secure routing protocols: SAODV and Ariadne. SAODV is secure routing protocol based on AODV routing protocol and Ariadne is secure routing protocol based on DSR routing protocol. We also compared the performance of SWBAODV with WBAODV performance as well.

We used the following five well-known ad hoc network performance metrics in the evaluation of SWBAODV, SAODV, Ariadne and WBAODV routing protocols.

5.3.1 Average End-to-End Delay

This is the average delay between, sending the data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes and retransmission delays at the MAC layer. It includes only all the packets that are correctly received. Lost packets are obviously not included in this measurement since their packet delay is infinity. The following equation is used to calculate this metric:

$$AED = \frac{\sum_{i=0}^{n} Time\ Packet\ Received_i - Time\ packet\ sent_i}{Total\ Numbe\ of\ Packets\ Received}$$

Where ‘n’ is the total number of packets. A higher value of end-to-end delay means that the network is congested and hence the routing protocol doesn’t perform well.

Figures (5.1) and (5.2) show the average end-to-end delay of SWBAODV, SAODV, Ariadne and WBAODV routing protocols with different number of mobile nodes and mobility speeds, respectively. As shown in figures (5.1) and (5.2), the average end-to-end delay increased as the number of mobile nodes or the mobility speed increased, because when number of nodes or mobility increases then more route discovery will be launched thus more latency before sending data packets .

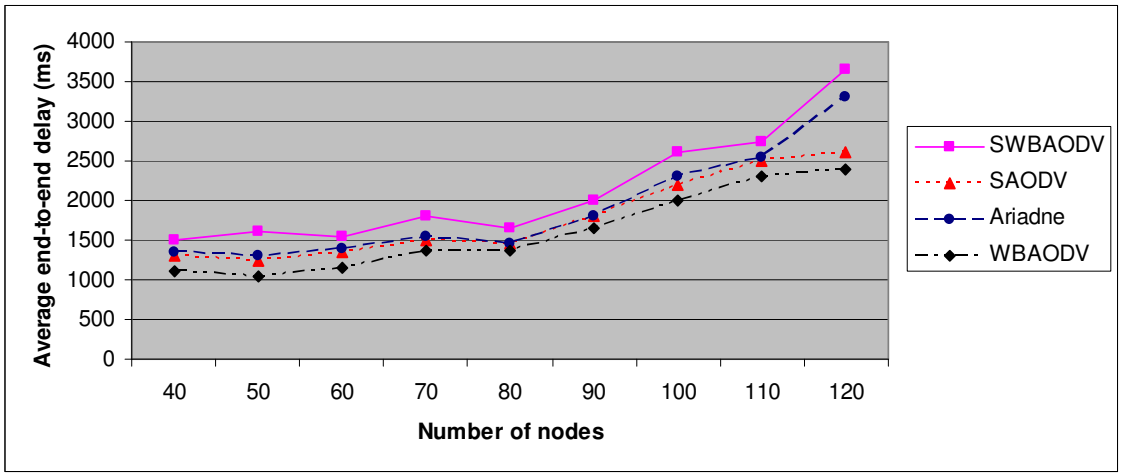

Figure (5.1): Average end-to-end delay versus number of nodes with 10 m/s

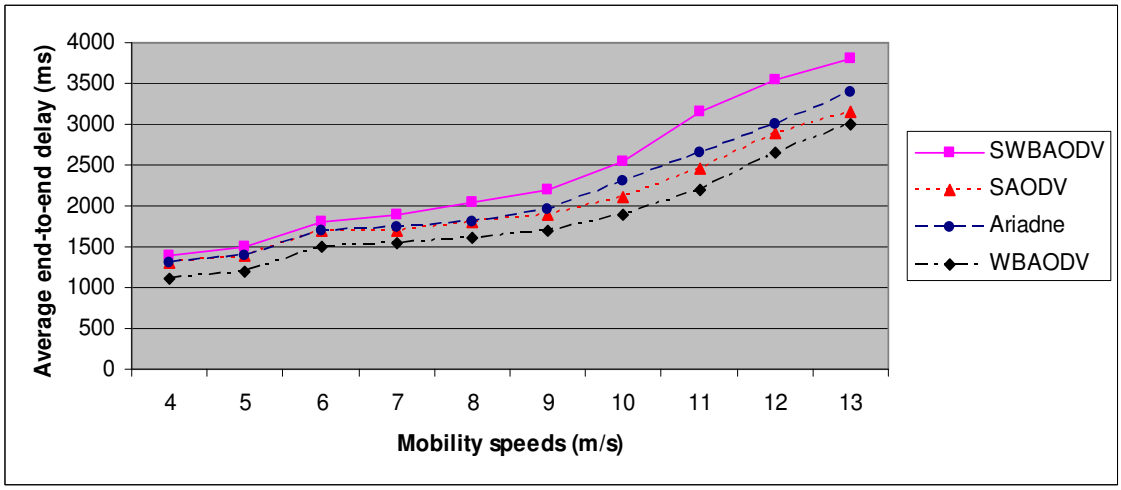

Figure (5.2): Average end-to-end delay versus mobility speeds with 50 nodes

The average end-to-end delay for SWBAODV is higher than that for SAODV and Ariadne. This is because SWBAODV have extra mechanism to select a path and it is also possible that SWBAODV select a longer hop route since it has to consider the stability problem. In addition, SAODV and Ariadne only select the shortest path or fastest transmission path. The extra mechanism in SWBAODV to select the path that increased the delay include that every intermediate node receives the RREQ packet will compute the weight using the weight function before broadcasts it to its neighbors, also only the destination can be reply to the RREQ packet and the destination will wait for certain interval to obtain all feasible paths before reply , but in other AODV-based secure routing protocols any intermediate node that know the fresh route to destination can reply and no any computations are needed.

Also the average end-to-end delay for SWBAODV is higher than that for WBAODV and this because SWBAODV used some cryptographic primitives which didn't exist in WBAODV like digital signature with time stamp and hash chains which considered being costly and increased the end-to-end delay, but these primitives are important and essential to secure routing messages. Another fact that SWBAODV used monitoring procedures and temporal leash test which are done node-by-node along the routing path which increased the total end-to-end delay. Finally although all the latter things which increased the delay, but the difference between SWBAODV, WBAODV, SAODV and Ariadne routing protocols in delay is still acceptable and not very high.

5.3.2 Packet Delivery Ratio

Also called throughput which is the ratio of the number of data packets successfully received by a destination over the number of data packets delivered by the corresponding source both at the application layer. Packets that are sent but not received

are lost in the network due to malicious drops, route failures, congestion, and wireless channel losses. The following equation is used to calculate this metric:

$$PDF = \frac{No\ of\ Packets\ Received\ by\ destination}{No\ of\ Packets\ Sent\ by\ Source}$$

This estimate gives us an idea of how successful the protocol is in delivering packets to the application layer. A high value of this ratio indicates that most of the packets are being delivered to the higher layers and is a good indicator of the protocol performance. Figures (5.3) and (5.4) show the packet delivery ratio of SWBAODV, SAODV, Ariadne and WBAODV routing protocols with different number of mobile nodes and mobility speeds, respectively.

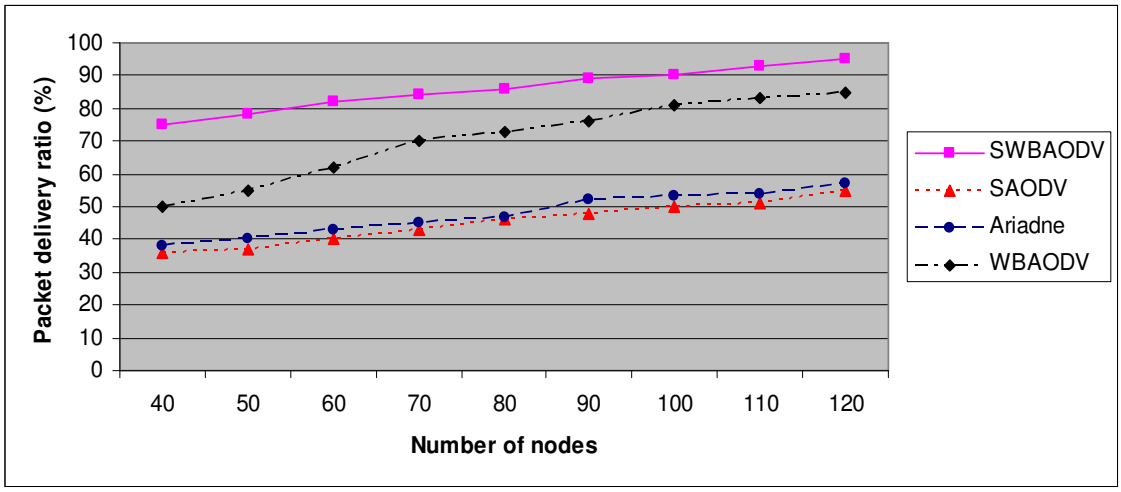

Figure (5.3): Packet delivery ratio versus number of nodes with 10 m/s

We can observe that SWBAODV transmits and receives more data packet than SAODV and Ariadne. This is because SAODV and Ariadne path may broken easily, but SWBAODV will always choose the most stable path, the chance of link breakage for SWBAODV is lower than that for SAODV and Ariadne since SAODV and Ariadne didn't consider the stability of the selected path.

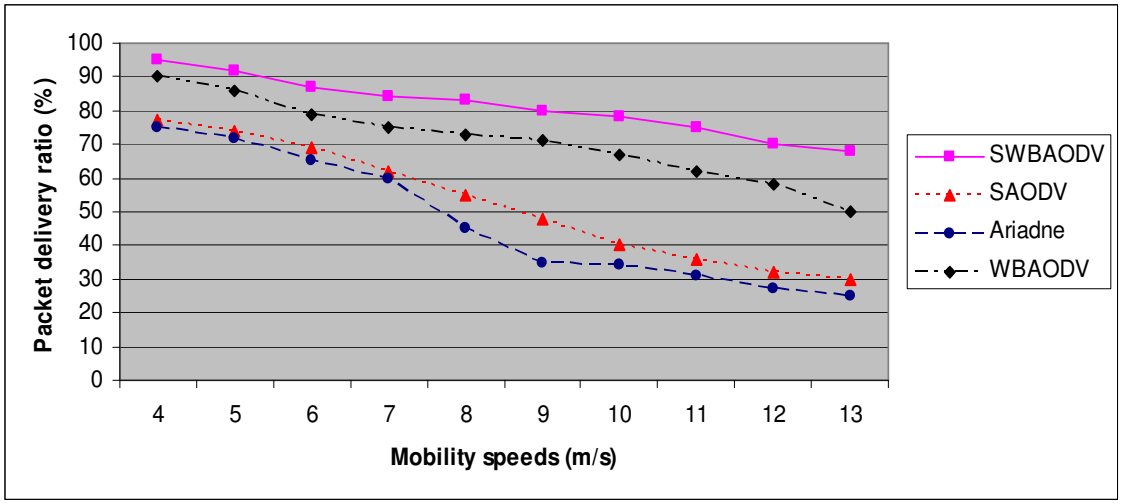

Figure (5.4): Packet delivery ratio versus mobility speeds with 50 nodes

Also we can observe that there is a big difference in the packet delivery ratio between SWBAODV and the rest of routing protocols in figures (5.3) and (5.4). This because SWBAODV used many security schemes to monitor, detect, isolate misbehaving nodes and cope many dangerous routing attacks in MANET. Such schemes which didn't exist in SAODV, Ariadne and WBAODV routing protocols will prevent malicious nodes to drop control packets or tunnel them and that at the end will cause to transmit and receive more data packets.

5.3.3 Number of Packets Drop

The total number of packets dropped during routing. It also defined as the packets that are dropped in the network due to malicious drops, route failures, congestion, and wireless channel losses. This estimate gives us an idea of how successful the protocol is in delivering packets to the application layer. A low value of this ratio indicates that the most of the packets are being delivered to the higher layers and is a good indicator of the protocol performance.

Figures (5.5) and (5.6) show the number of packets drop of SWBAODV, SAODV, Ariadne and WBAODV routing protocols with different number of mobile

nodes and mobility speeds, respectively. As shown in figures (5.5) and (5.6), the number of packets drop increased as the number of mobile nodes or the mobility speed increased. Because SWBAODV always chooses the most stable route for transmission that reduces the number of packets dropped, so the number of call dropping of SWBAODV is lower than that of SAODV and Ariadne.

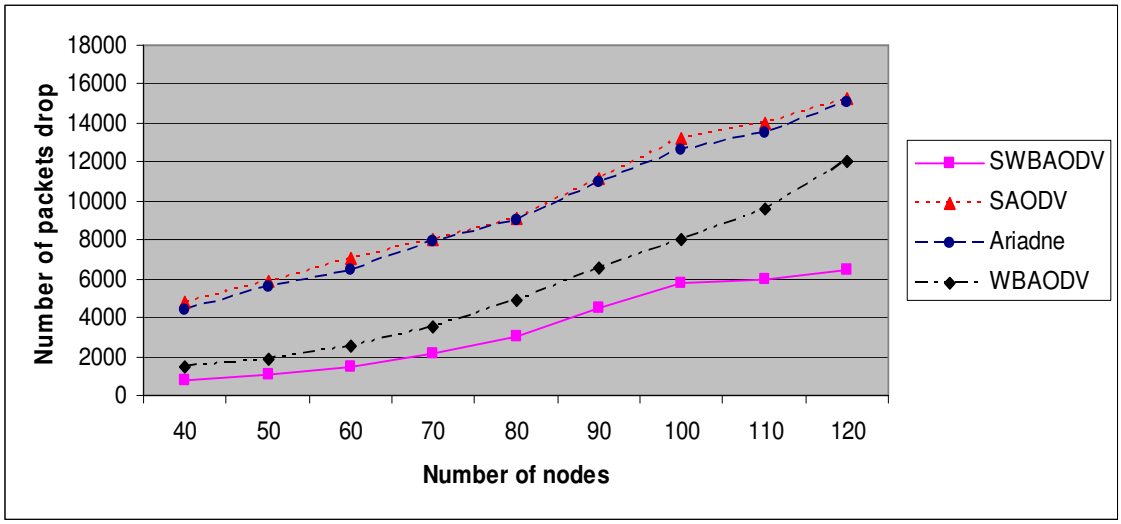

Figure (5.5): Number of packets drop versus number of nodes with 10 m/s

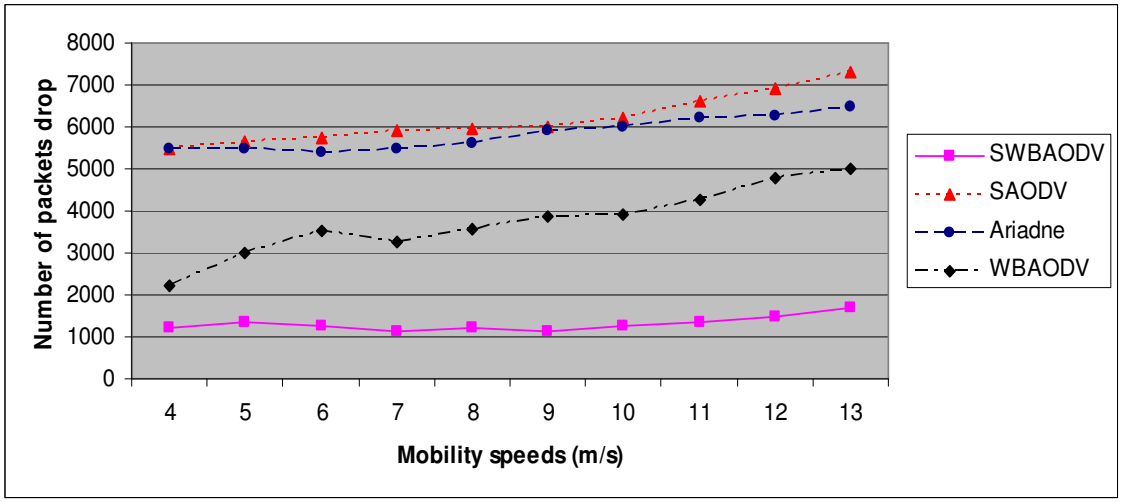

Figure (5.6): Number of packets drop versus mobility speeds with 50 nodes

We can also observe that there is a big difference in the number of packets drop between SWBAODV and the rest of routing protocols in figures (5.5) and (5.6). This because SWBAODV used many security schemes to monitor, detect, isolate

misbehaving nodes and cope many dangerous routing attacks in MANET. Such schemes which didn't exist in SAODV, Ariadne and WBAODV routing protocols will prevent malicious nodes to drop control packets or tunnel them and that at the end will cause to reduce the number of dropped data packets. Another reason that SWBAODV decreased the number of dropped packets is using the flooding attack prevention scheme which will prevent malicious nodes to flood the network of useless RREQ packets and that will lead to reduce the congestion over the links.

5.3.4 Routing Packets Overhead

It can be defined as the total number of routing packets transmitted during the simulation. For packets sent over multiple hops, each transmission of the packet at each hop counts as one transmission. Data packets aren't included in the calculation of this metric. This estimate gives us an idea of how successful the protocol can provide stable routing paths and reduces the links congestion. A low value of this measure indicates that more stability of routing paths and less congestion in the network which is considered as a good indicator of the protocol performance.

Figures (5.7) and (5.8) show routing packets overhead of SWBAODV, SAODV, Ariadne and WBAODV routing protocols with different number of mobile nodes and mobility speeds, respectively. As shown in figures (5.7) and (5.8), the routing overhead increased as the number of mobile nodes or the mobility speed increased. Since the physical area remains the same, a small number of mobile hosts mean a lower host density. In general, the routing overhead of Ariadne and SAODV increased faster than the routing overhead of SWBAODV when the number of hosts increased. This is because Ariadne and SAODV just select the shortest path for routing. However, SWBAODV always selects the most stable route (the route with the maximum weight

value) for routing. Therefore, the overhead of SWBAODV is lower than that of Ariadne and SAODV.

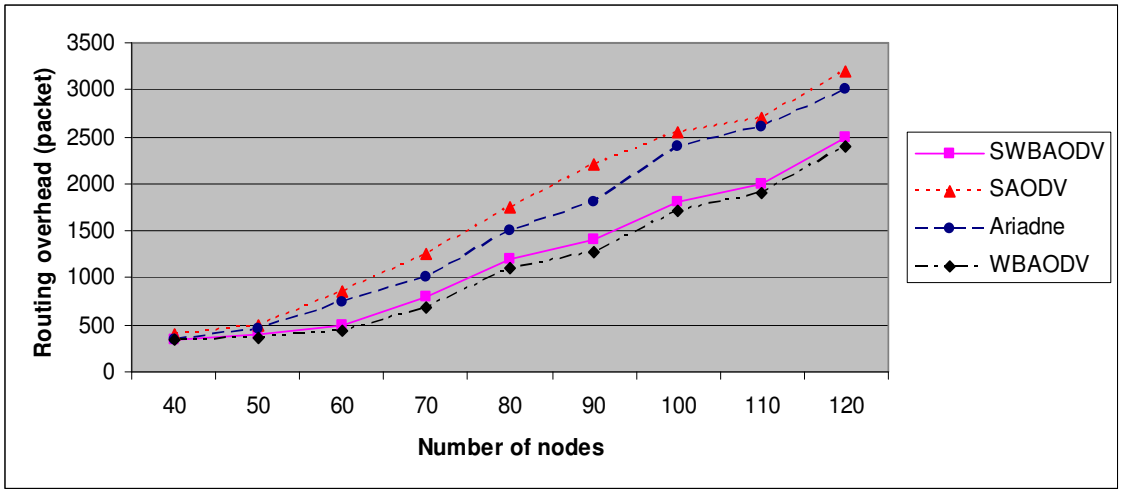

Figure (5.7): Routing packets overhead versus number of nodes with 10 m/s

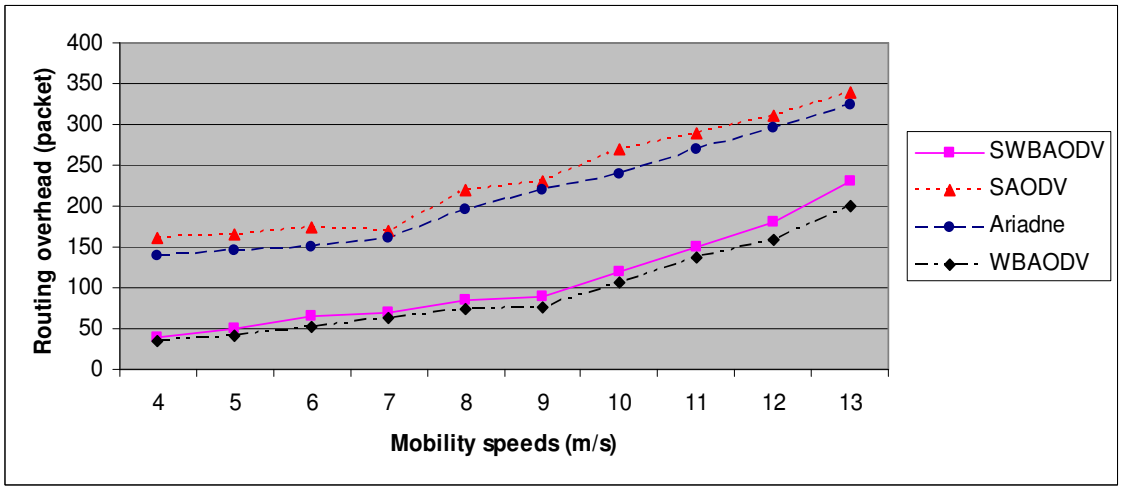

Figure (5.8): Routing packets overhead versus mobility speeds with 50 nodes

Also in general, the routing overhead of Ariadne and SAODV increased faster than the routing overhead of SWBAODV when the roaming speed increased. This because the routing path is easier to be broken when the speed of the mobile hosts is faster. In addition, the number of rebroadcasts will increase. Therefore, the overhead is higher as a result. Although SWBAODV uses some special packets like Two-hop ACK, WREQ, WREP, ACREQ, ACREP and AC which are used as a part of the control

packet dropping prevention scheme to monitor, detect and isolate the misbehaving nodes along the route path and over the network, but the overhead is not an important issue for this kind of packets, since their number is low in comparison with the number of main routing packets.

The routing overhead of SWBAODV is approximately similar to the routing overhead of WBAODV routing protocol. The small difference between them in routing overhead is due to that SWBAODV uses some special packets which didn't exist in WBAODV and this leads to increase the routing overhead in SWBAODV about that in WBAODV routing protocol.

5.3.5 Average Power Consumption

We can define the average consumed power as the following equation:

$$average\_power = \sum_{i=1}^{n} \frac{PC_i}{n}$$

Such that PC_i is the power consumed by node i during the simulation. This estimate gives us an idea of how the protocol affect on the power available in the nodes' battery. A low value of this measure indicates that less processing and transmissions which is considered as a good indicator of the protocol performance.

Figures (5.9) and (5.10) show the average power consumption of SWBAODV, SAODV, Ariadne and WBAODV routing protocols with different number of mobile nodes and mobility speeds, respectively. As shown in figure (5.9) the average power consumption of SWBAODV increased faster than the average power consumption of SAODV and Ariadne when the number of hosts increased. This is because SWBAODV uses combination of security mechanisms to cope different types of attacks and also uses the weight-based routing strategy to select the stable path which in result there is a

large amount of processing at each node. On the other hand because SAODV and Ariadne always selects the shortest path and didn't use any of these security mechanisms which exist in SWBAODV, they will consume power lower than of that in SWBAODV.

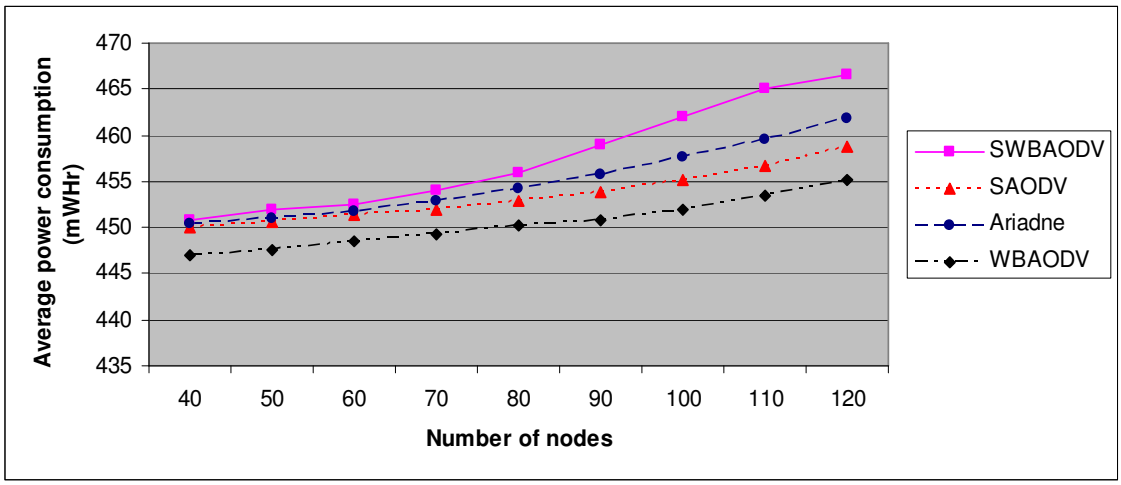

Figure (5.9): Average power consumption versus number of nodes with 10 m/s

In figure (5.10) we can observe that the average power consumption of SWBAODV decreased faster than the average power consumption of SAODV and Ariadne when the roaming speed increased. This is mainly due to the increasing of packets lost when the mobility is raised. Because of the stability of SWBAODV these lost packets is lower than of that in SAODV and Ariadne, so SWBAODV consumes power lower than them in high mobility. In general the small difference in the power consumption between SAODV, Ariadne and SWBAODV in high mobility is due to the overhead which indicates that the cost of the control packets added by the latter (overhead) is minor.

The average power consumption of WBAODV is lower than that of SWBAODV and this can be explained by that SWBAODV uses many security mechanisms to cope many routing attacks which consume the node's battery faster than in WBAODV routing protocol which didn't consider the security problem in MANET.

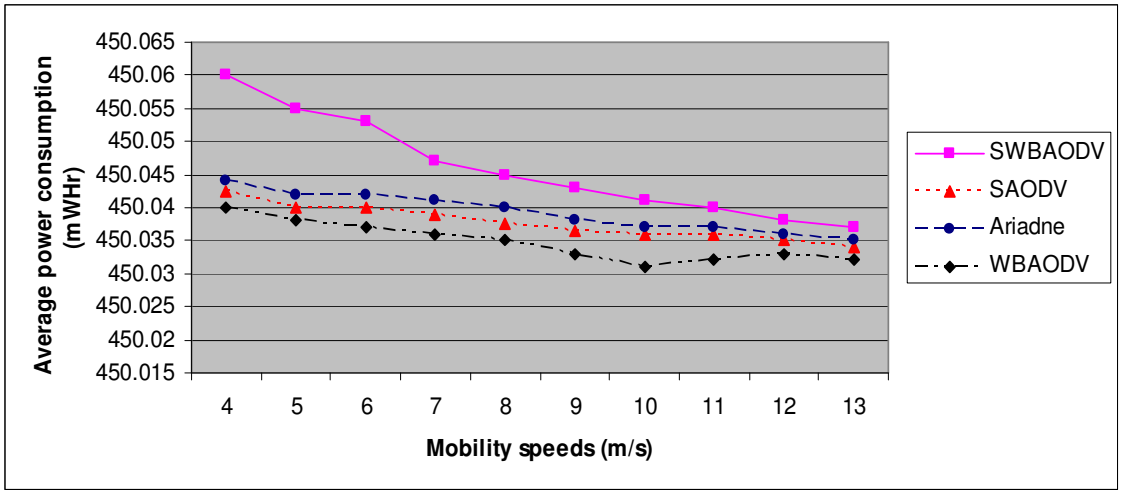

Figure (5.10): Average power consumption versus mobility speeds with 50 nodes

Chapter 6

Epilogue

6.1 Conclusion

In this thesis we proposed a new secure routing protocol in MANET which we called Secure Weight-Based Ad hoc On-demand Distance Vector (SWBAODV) routing protocol. SWBAODV is an on-demand routing protocol, but the main difference between SWBAODV and other on demand routing protocols is that SWBAODV uses the weight-based routing strategy which selects a stable routing path by maximizing the weight among all the feasible paths. The route selection is based on the weight value of each feasible path. In a feasible path, the less weight value represents less reliability. It also represents higher mobility of each node in the path. SWBAODV always selects the most stable path for routing which it has the maximum weight value.

We also added to SWBAODV many security mechanisms and primitives which cooperated well together to enhance its immunity against most common routing attacks in MANET. The results of security analysis of SWBAODV and six of secure routing protocols in MANET against these attacks show that all the six secure routing protocols in MANET success to prevent some attacks and failed in another, but SWBAODV success to prevent or mitigate all of them. Also SWBAODV success to satisfy all the standard security goals.

We built SWBAODV and compared its performance with two of famous on-demand ad hoc secure routing protocols (SAODV and Ariadne) and WBAODV routing protocol. These four routing protocols were evaluated through JiST/SWAN simulator.

We subjected these four routing protocols against extensive simulations with ad hoc network's performance metrics like average end-to-end delay, packet delivery ratio (throughput), number of packets drop, routing overhead and the average power consumption. These metrics was chosen due to they were well-known in showing the routing performance of the selected routing protocols. Experimental results show that the SWBAODV outperforms SAODV and Ariadne in throughput, the number of packets drop and routing overhead especially in the high mobility environment. Although SWBAODV increases the average end-to-end delay and the average power consumption, but this is the penalty of using the weight-based routing strategy and many combined security mechanisms to provide routing stability and coping many attacks which SAODV and Ariadne are vulnerable to them.

The difference between SWBAODV, SAODV and Ariadne in delay and power consumption is still acceptable and get closer in high mobility environment due to the stability of SWBAODV which is not exist in SAODV and Ariadne. Because one of the main properties of MANET is high mobility, so we can say that SWBAODV has better performance than other secure on-demand routing protocols.

6.2 Future Work and Recommendations

Research in the area of ad hoc secure routing protocols is still actively done. Due to the time limitations and code availability the current work was only focused on evaluating SWBAODV with two secure routing protocols in MANET: SAODV and Ariadne with some selected performance metrics. The performance evaluation of SWBAODV with other ad hoc secure routing protocols which are discussed in this thesis work with some more performance metrics and studying the limitation of SWBAODV performance in large MANET will be considered as future research work.

References

[1] S. Basagni, M. Conti, S. Giordano, Stojmenovi, and Cacute, in “Mobile Ad Hoc Networking,” Wiley-IEEE Press, pp.1-33, 275-300, 330-354, September 2004.

[2] C. Siva, R. Murthy, and B.S. Manoj, in “Ad Hoc Wireless Networks, Architecture and Protocols,” Pearson Education, pp. 321-386, 473-526, 2004.

[3] E. M. Royer, and C.K. Toh, “A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks,” IEEE Personal Communications Magazine, pages 46-55, April 2001.

[4] X. Hong, K. Xu, and M. Gerla, “Scalable Routing Protocols for Mobile Ad Hoc Networks,” Computer Science Department, University of California, Los Angeles, August 2002.

[5] T. Lin, S. F. Midkiff, and J.S. Park, “A Framework for Wireless Ad Hoc Routing Protocols,” Bradley Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg Virginia, 2003.

[6] V.Sumathy, P. Narayanasamy, J.James and S.Kanimozhi, “THROUGHPUT MAXIMIZATION ROUTING IN MOBILE AD-HOC NETWORK BY LINK BREAK PREDICTION,” Academic Open Internet Journal, Volume 16, 2005.

[7] Z. Kai, W. Neng, and L. Ai-fang, “A new AODV based clustering routing protocol,” Wireless Communications, Networking and Mobile Computing, on Proceedings of International Conference, IEEE, Volume 2, Issue 23-26, PP. 728 – 731, Sept. 2005.

[8] Wang, N.C., Y.F. Huang and J.C. Chen, "A stable weight-based on-demand routing protocol for mobile ad hoc networks," Information Sciences Vol. 177, Issue 24, pp. 5522-5537, December 2007.

[9] K. Khamforoosh, A. M. Rahmani, A. Sheikh Ahmadi, “A new multipath AODV routing based on distance of nodes from the network center,” Communications,

Propagation and Electronics, MIC-CPE, on Mosharaka International Conference, IEEE, Volume 10, Issue 6-8, pp. 1– 5, March 2008.

[10] S. Tabatabaei, M.A. Jamali, “A stable weight-based Routing Algorithm to Increase Throughput in Mobile Ad hoc Networks,” Mobile computing, IEEE, 2009.

[11] M.G. Zapata, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing," IETF Internet Draft, draft-guerrero-manet-saodv-00.txt, August 2001.

[12] L. Jun, L. Zhe, L. Dan, and L. Ye, “A security enhanced AODV routing protocol based on the credence mechanism,” Wireless Communications, Networking and Mobile Computing, on Proceedings of International Conference, IEEE, Volume 2, Issue 23-26, pp. 719 – 722, Sept. 2005.

[13] D. Djenouri, O. Mahmoudi, M. Bouamama, D. Llewellyn-Jones, and M. Merabti, “On Securing MANET Routing Protocol Against Control Packet Dropping,” on Pervasive Services, IEEE International Conference, Istanbul, ISBN: 1-4244-1325-7, pp. 100-108, 15-20 July 2007.

[14] N. Bhalaji, and A.Shanmugam, “ASSOCIATION BETWEEN NODES TO COMBAT BLACKHOLE ATTACK IN DSR BASED MANET,” on Mobile Computing, IEEE, 2009.

[15] M.M. Ibrahim, N. Sadek, and M. El-Banna, “Prevention of Flooding Attack in Wireless Ad-Hoc AODV-based networks using Real-time Host Intrusion Detection,” on Mobile Computing, IEEE, 2009.

[16] C. E. Perkins, E. M. Belding-Royer, and I. Chakeres, "Ad Hoc On Demand Distance Vector (AODV) Routing," IETF Internet draft, draftperkins-manet-aodvbis-00.txt, October 2003.

[17] C. E. Perkins, E. M. Belding-Royer, and S. Das, "Ad Hoc On Demand Distance Vector (AODV) Routing," RFC 3561, IETF Network Working Group, July 2003.

[18] C. Y. Chiu, H. K. Wu, and G. H. Chen, "Stability Aware Cluster Routing Protocol for Mobile Ad Hoc Network," Proceedings of the ninth International Conference on Parallel and Distributed System (ICPADS 2002), December 2002.

[19] T. G. Griffin, F. B. Bruce, and G. Wilfong,, "The Stable Paths Problem and Interdomain Routing,," IEEE/ACM Transactions on networking, Vol. 10, No. 2, pp. 232-243, April 2002.

[20] W. I. Kim, D. H. Kwon, and Y. J. Suh, "A Reliable Route Selection Algorithm Using Global Positioning Systems in Mobile Ad Hoc Networks," Proceeding of IEEE International Conference on Communications (ICC 2001), pp. 3191-3195, June 2001.

[21] H. EL_afandi, “An Intelligent Wireless Ad hoc Routing Protocol,” University of Wisconsin, Milwaukee, 2006.

[22] D. Espes, Z. Mammeri, “Routing Algorithm to Increase Throughput in Ad hoc Networks,” International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies ,2006.

[23] O. C. His, A. Abdullah, "Performance evaluation of stable weight-based on demand routing protocol for mobile Ad hoc Network," Journal of Computer Science Vol. 10, pp. 732-737, October 2009.

[24] H. Deng, W. Li, and D. P. Agarwal, “Routing Security in Wireless Ad Hoc Networks,” University of Cincinnati, IEEE Communications magazine, Vol.40, no.10, 2002.

[25] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile ad hoc networks: Challenges and solutions," Wireless Communications, IEEE, vol. 11, pp. 38-47, February 2004.

[26] W. Stallings,” Network Security Essentials: Security Attacks,” Prentice Hall, pp. 2-17, 2000.

[27] A. Habib, M. H. Hafeeda, and B. Bhargava, "Detecting Service Violation and DoS Attacks," In Proc. Network and Distributed System Security Symposium, 2003.

[28] Y.C. Hu, A. Perrig, and D.B. Johnson, “Wormhole Attacks in Wireless Networks,” In IEEE JSAC, Vol. 24, No. 2, pp. 370-380, February 2006.

[29] Y. Hu, D.B. Johnson, and A. Perrig, “Secure Efficient Ad hoc Distance vector routing,” in the Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and applications (WMCSA’02), 2002.

[30] S. A. Mohammed, "Evaluation of Mobile Ad hoc Secure Routing Protocols With case studies on Attack Patterns and Simulation," M.S. thesis, Dept. Computer and Systems Sciences, Royal Institute of Technology (KTH), Stockholm, Sweden, February 2006.

[31] M. G. Zapata, " Secure Ad hoc On-Demand Distance Vector Routing,," ACM SIGMOBILE Mobile Computing and Communication Review, Vol. 6, No. 3, July 2002.

[32] Y. Lin, A. Rad, V. Wang and J. Song, "Experimental comparisons between SAODV and AODV routing protocols," International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems, Proceedings of the 1st ACM workshop on Wireless multimedia networking and performance modeling, Montreal, Quebec, Canada, pp. 113 – 122, 2005.

[33] D. Djenouri and N. Badache, "A novel approach for selfish nodes detection in Manets: Proposal and petri nets based modeling". In The 8th IEEE International Conference on Telecommunications (ConTel’05), pages 569–574, Zagreb, Croatia, June 2005.

[34] D. Djenouri and N. Badache, "Testimony-based isolation: New approach to overcome packet dropping attacks in Manet". In The 7th Postgraduate Symposium on Convergence of Telecommunications, Networking and Broadcasting (PgNet'06), pages 114–119, John Moors University, Liverpool, UK, June 2006.

[35] P. Yi, Z. Dai, S. Zhang and Y. Zhong, "A New Routing Attack in Mobile Ad hoc Networks," International Journal of Information Technology, Vol. 11, No. 2, pp. 83-94, 2005.

[36] Y. C. Hu, A. Perrig, and D. B. Johnson, " Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, Vol. 3, pp. 1976-1986, April 2003.

[37] I. D. Chakeres, and E. M. Belding-Royer, "AODV Routing Protocol Implementation Design," Proceedings of the International Workshop on Wireless Ad Hoc Networking (WWAN), Tokyo, Japan, March 2004.

[38] E.M. Royer, and C. E. Perkins, "An Implementation Study of the AODV Routing Protocol," Proceedings of the IEEE Wireless Communications and Networking Conference, Chicago, IL, September 2000.

[39] URL: "http://jist.ece.cornell.edu/", July 2009.

[40] URL: "http://jist.ece.cornell.edu/docs/040421-swans-aodv.pdf", July 2009.

[41] P. Michiardi and R. Molva, "Simulation-based analysis of security exposures in mobile ad hoc networks," In Proceedings of European Wireless Conference, 2002.

[42] G. Acs, L. Buttyan, and I. Vajda, "Provably secure on-demand source routing in mobile ad hoc networks," IEEE Transactions on Mobile Computing, Vol. 5, No. 11. pp.1533–1546, 2006.

[43] K. Balakrishnan, J. Deng, and P. K. Varshney, "Twoack: preventing selfishness in mobile ad hoc networks," In The IEEE Wireless Communications and Networking Conference(WCNC'05), pages 2137– 2142, New Orleans, LA, USA, March 2005.

[44] S. Buchegger and J.-Y. Le-Boudec, "A robust reputation system for p2p and mobile ad-hoc networks," In Second Workshop on the Economics of Peer-to-Peer Systems, Harvard university, Cambridge, MA, USA, June 2004.

[45] L. Buttyan and I. Vajda, "Towards provable security for ad hoc routing protocols," In The ACM Workshop on Security in Ad Hoc and Sensor Networks SASN04, Washington DC, October 2004.

[46] S. Capkun, L. Buttyan, and J.-P. Hubaux, "Self-organized public-key management for mobile ad hoc networks," IEEE Transactions on Mobile Computing, Vol. 2, No. 1, pp.52–64, January 2003.

[47] B. Dahill, B. N. Levine, E. Royer, and C. Shields, "Aran: A secure routing protocol for ad hoc networks," Technical Report UMass Tech Report 02-32, University of Massachusetts, Amherst, 2002.

[48] B. David and A. David, "Dynamic source routing in ad hoc wireless networks," In Mobile Computing, volume 353, pages 153–181, Kluwer Academic, imielinski and korth edition, 1996.

[49] D. Djenouri and N. Badache, " New power-aware routing for mobile ad hoc networks," The International Journal of Ad Hoc and Ubiquitous Computing (Inderscience Publisher), Vol.1, No.3, pp.126–136, 2006.

[50] D. Djenouri, L. Khalladi, and N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," IEEE Communications Surveys, Vol.7, No.4, pp.2–28, 2005.

[51] D. Djenouri, N. Ouali, A. Mahmoudi, and N. Badache, "Random feedbacks for selfish nodes detection in mobile ad hoc networks," In The 5th IEEE International Workshop on IP Operations and Management, IPOM'05, number 3751, In LNCS, pages 68–75, Springer-Verlag GmbH, Barcelona, Spain, October 2005.

[52] S. Doshi and T. Brown, "Minimum energy routing schemes for a wireless ad hoc network," In The 21st IEEE Annual Joint Conference on Computer Communications and Networking, INFOCOM'02, New York, USA, 2002.

[53] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne:: a secure on-demand routing protocol for ad hoc networks. In The 8th annual international conference on Mobile computing and networking, MobiCom '02, pages 12–23. ACM Press, 2002.

[54] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," In ACM Mobile Computing and Networking, MOBICOM 2000, pages 255–65, Boston, MA, USA, 2000.

[55] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," In The 6th IFIP Communication and Multimedia Security Conference, Portoroz, Slovenia, September 2002.

[56] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," In The SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, CNDS02, San Antonio, Texas, 2002.

[57] S. Yi, P. Naldurg, and R. Kravets, "Security-aware ad hoc routing for wireless networks," In The ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC01), Long Beach, CA, October 2001.

[58] I. Stamouli, P. G. Argyroudis, and H. Tewari, "Real-time Intrusion Detection for Ad hoc Networks," In Proc. 16th IEEE Int'l. Sym. on a World of Wireless Mobile and Multimedia Networks (WoWMoM'05), pp. 374-380, 2005.

[59] R. Barr, " JiST—Java in Simulation Time: User Guide and Tutorial," Sept. 2003.

[60] C. Lin, "AODV Routing Implementation for Scalable Wireless Ad-Hoc Network Simulation (SWANS)," Available at: "http://jist.ece.cornell.edu/docs/040421-swans-aodv.pdf", June 2010.