DEVELOPING PREVENTIVE MESUREMENTS AGAINST ATTACKS ON WIRELESS NETWORKS

GHAIDAA AHMED ALI

FEBRUARY 2017

DEVELOPING PREVENTIVE MESUREMENTS AGAINST ATTACKS ON WIRELESS NETWORKS

A THESIS SUBMITTED TO

THE GRADUATE SCHOOL OF NATURAL AND APPLIED

SCIENCES OF

ÇANKAYA UNIVERSITY

BY

GHAIDAA AHMED ALI

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF MASTER OF SCIENCE IN THE DEPARTMENT OF

COMPUTER ENGINEERING

FEBRUARY 2017

Title of the Thesis: **Developing Preventive Measurements against Attacks on Wireless Networks**

Submitted by **Ghaidaa Ahmed ALI**

Approval of the Graduate School of Natural and Applied Sciences, Çankaya University

Prof. Dr.Halil Tanyer EYYUBOGLU

Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science

Prof.Dr. Muslim BOZIGIT

Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Prof. Dr. Shaimaa HAMEED

Co-Supervisor

Prof. Dr. Reza HASSANPOUR

Supervisor

Examination Date: 01.02.2017

Examining Committee Members

Assist. Prof. Dr. Reza HASSANPOUR (Çankaya univ.)

Assist. Prof. Dr. Abdul Kadir GÖRÜR (Çankaya univ.)

Assist. Prof. Dr. Kasım ÖZTOPRAK (Karatay univ.)

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: Ghaidaa ALI

Signature:

Date: 01.02.2017

Abstract

Developing Preventive Measurements against Attacks on Wireless Networks

Ghaidaa Ahmed Ali

M.Sc., Department of Computer Engineering

Supervisor: Assist. Prof. Dr. Reza Hassanpour

Co-supervisor: Assist. Prof.Dr. Shaimaa Hameed Shaker

February 2017

Abstract

Wireless Sensor Networks (WSN) and Ad Hoc networks are being using in different applications and fields of our life in the modern era. They are used in the military, medical, industrial, disaster relief, and commercial applıcatıons. Security is an important challenge in the wireless networks. Most of the wireless networks are susceptible to different attacks. In this study we address Sybil attack which uses multiple identities for a node to create the illusion that these identities come from multiple nodes. In this thesis, we propose a method to detect and prevent Sybil attacks. In our method, we consider WSN application in vehicular networks (VANET) where we detect Sybil attack without knowing the identity of the malicious node which preserves the user privacy as well. The proposed method is simulated in NS2, a widely used open source network simulator. The results are compared with the realistic test case conducted by the centralized authority DMV in terms of the detection rate and overheads.

Table of Contents

LIST OF FIGURES

Figures

LIST OF TABLES

Tables

General Introduction

Chapter 1

1.1 Overview:

The wireless networks are one of the applications in the modern era, it consists small sensors in size and communicate unconnected in short distances. It is characterized by low-cost, low-power, and multifunctional. The work of sensor nodes, it is for sensing data then processing the data and communicating components. The idea of wireless networks is based on cooperative effort of a large number of nodes. As appears in the figure (1-1) [1] [2].

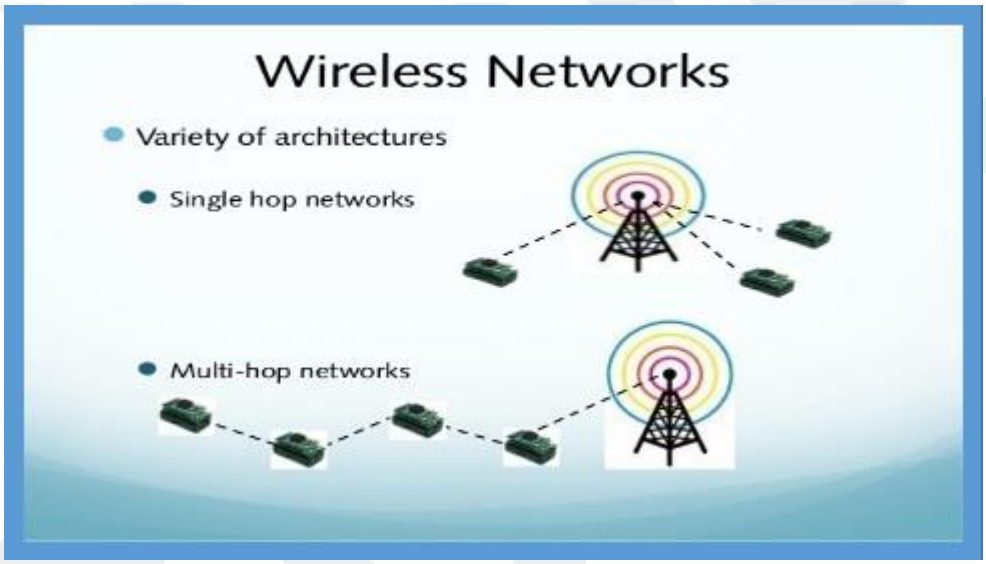


Figure (1-1) Wireless Networks [1]

There are several kinds of wireless networks like the Wireless Sensor Networks (WSN) and Ad Hoc Network etc… Wireless Sensor Network (WSN) is an arising technology which shows great promises for different applications both for the comprehensive public and the military [3]. WSNs are collection of sensor nodes that have capability to move. These nodes can exchange information and communicate with others in a free environment. Another type of wireless networks is ad hoc networks. Ad hoc networks are independent from central nodes, it is used in different applications as a personal area network, military police, homes networks, and disaster relief. The ad hoc networks consist of nodes that can connect to others with inconstant topology and in different location [4]. The major challenge in the wireless networks is security. The sensor nodes that are distributed in an uncontrolled environment have exposed the networks to

different types of attacks. The traditional security to prevent attacks is not an effective solution because of the power and the size of sensor nodes. Wireless networks make life easier, it makes things more comfortable. There are many attackers that can have an effect on WSN and Ad hoc networks. Sybil attack considers one of several attacks that can have an effect on networks. It is an attack that creates multiple identities from the same malicious node [3]. There are many methods used to prevent and detect Sybil attacks such as Public Key Cryptography, Privacy Preserving Detection Scheme and Detection using Neighboring Nodes. However, the fundamental of this thesis is to find the efficient techniques to detect and prevent Sybil attack [1][2][3][4].

1. 2 Previous Works:

There is a lot of research on the Sybil attack. This research found ways to appoint the attack and others to prevent this attack, but some of these ways are relatively difficult to process or they are applied in an impractical way. Some of these researches are included as following:

1. **Radio Resource Testing:**

   This method is assuming each physical entity has limited number of resources. This method is not viable to ad hoc networks. The attackers can use more computational resources than normal nodes [24].

2. **Public Key Cryptography**:

   This method is based on the central authority; it is responsible for giving certificates to each node. The node uses the certificate to authenticate itself. This method is unsuitable for large networks [9] [10].

3. **Privacy Preserving Detection Scheme:**

   It provides the pseudonyms to each node in the network in order to hide its information. The pseudonym nodes are hashed by a particular common value. These hash are stored in moveable server. This method is provided privacy. The nodes need to register themselves. This scheme is difficult to implement because the number of nodes cannot register every node [36].

4. **Detection Using Neighboring Nodes**:

   This scheme explain that every node participates in the detection of an attack on the network. Each node has different group of neighbors at a different time. If the vehicle

has same neighbors in different time this vehicle is considered an attack. This method is provided privacy [48].

5. **Timestamp Series Approach:**

This method is based on Road Side Unit (RSU); it is responsible for the timestamp. The timestamp to each node is signed digitally by RSU. If the node wants to send information to any other node, it must go to the RSU to give the timestamp. After getting the timestamp it sends message to other vehicles. This scheme does not work in complex [14]. [13].

1.3 The Goal of Thesis:

The aim of this thesis is finding method to prevent Sybil attack in practical manner. The goal has been achieved through the following:

1. Studying Sybil attack in (WSN and Ad hoc) networks.
2. Finding advantage and disadvantage of different types of algorithms to detect and prevent Sybil attack (WSN and Ad hoc).

1. 4 The Contributions of Thesis:

This thesis is focused on detect and prevent Sybil attack. The advantage and disadvantage of other mechanisms are found and are tested to approve the proposed method. The contributions of this thesis can be mentioned as follows:

- The proposed method is based on the privacy preserving to prevent Sybil attack.
- It is assumed each node communicate with others in multihop manner.
- The proposed method is considering the Department of Motor Vehicle (DMV) is an important part in the network that provides a **pool of keys**, the DMV is responsible for certificate authority.
- The key is distributed to each node. These keys are used to hide the node's information.
- The proposed method has created a wireless network in safe way

1.5 Thesis Structure:

This thesis consists of six chapters. The second chapter talks about a background of WSN and ad hoc networks along with their applications. There is also security requirement in wireless networks, attack models, Sybil attack, Sybil attack creation in wireless network, and types of Sybil attack. Chapter three discusses previous studies to detect and prevent Sybil attack and the advantage and disadvantage to each method. Chapter four discusses the proposed method in (VANET). Chapter five explains the simulation and results. Lastly, the conclusion and the future works will be in chapter six.

Chapter 2

Overview of WSN and Ad hoc Networks

2.1 Introduction:

The objective of this chapter is to explain what (WSN and Ad hoc) networks and how to apply them. Then, it explains attack models in wireless networks. Sybil attacks are penetrating in wireless networks.

2.2 The Features of Wireless Networks:

The wireless networks have mutual collaboration for information exchanges. Also, there are important challenges such as the following: [9]

1. This kind of network is fast-spreading and is able to self-organize.
2. A wireless network is short of pre-broadcast infrastructures, so a centralized network management solution is not suitable for such an environment.
3. Wireless devices usually use batteries as their power supply, thus do not use complex security.
4. Because the nature of wireless channels that the data privacy needs to protect.
5. The cooperation between nodes is necessary in wireless links because have short transmission ranges.
6. Wireless networks often are not in fixed form so you need a strong security to protect it.

2.3 The Wireless Sensor Networks (WSN):

WSN is a new technology, it is considered a good technology. WSN creates meaningful solutions for commercial applications. This network has a number of applications at various fields of modern science. The architecture of WSN contents of small and lightweight nodes that is distributed in the network. All the sensor nodes are similar to computers with processing unit. It is limited in power and in memory. WSN is applied in different environment as in temperature and pressure etc. The power source to the nodes is a battery. There are many attacks exposed to WSN. As shown in figure (2.1) the architecture of WSN [17] [18].

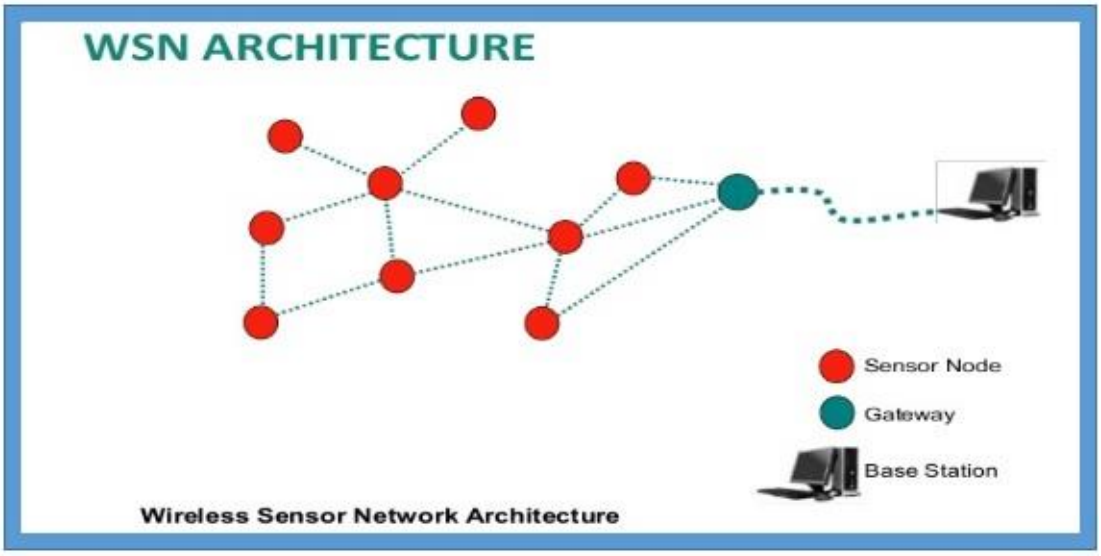


Figure (2.1) Wireless sensor network form [17]

2. 4 Issues of WSN:

The WSN network is affected by many issues. Here are some of the issues. [50]

1.The Energy Efficiency:

Limited battery size in the nodes of WSNs. These nodes used to use the battery for different functions as for sensing and communicating purpose. The energy is considered one of the serious issues.

2. The Size of Networks:

In general, the number of nodes in WSN network can be larger than ad hoc network.

3. The Density of Distribute:

The distribution of nodes in WSN differs from domain of application.

4. The Data and The Information Fusion:

It denotes to the collection of all packets before the expulsion of it.

Information fusion: It aims to process the sensed data at the intermediate nodes then it relaying the outcome to the monitor node.

5. The Traffic Deployment:

The communication traffic pattern differs with the domain of application in WSN.

2.5 The Routing Protocols in WSN:

In WSN the routing differs from the traditional routing that is in a fixed network. Because it does not have infrastructure and the links are unreliable. So, the nodes may be fail. There are many routing protocols developed for WSNs. It is divided into seven groups as appears in the table (2.1) [40].

Table (2.1) The Routing Protocols to WSNs [40]

Category	Representative Protocols
Location-based Protocols	MECN, SMECN, GAF, GEAR, Span, TBF, BVGF, GeRaF
Data-centric Protocols	SPIN, Directed Diffusion, Rumor Routing, COUGAR, ACQUIRE, EAD, Information-Directed Routing, Gradient Based Routing, Energy-aware Routing, Information-Directed Routing, Quorum-Based Information Dissemination, Home Agent Based Information Dissemination
Hierarchical Protocols	LEACH, PEGASIS, HEED, TEEN, APTEEN
Mobility-based Protocols	SEAD, TTDD, Joint Mobility and Routing, Data MULES, Dynamic Proxy Tree-Base Data Dissemination
Multipath-based Protocols	Sensor-Disjoint Multipath, Braided Multipath, N-to-1 Multipath Discovery
Heterogeneity-based Protocols	IDSQ, CADR, CHR
QoS-based protocols	SAR, SPEED, Energy-aware routing

2.6 Applications of WSN:

WSNs have many applications in different fields. This section is listed applications of WSN [18].

1. **The Military Applications:**

There are several applications of WSN in military field that including the control of the battlefield and monitor systems of intelligent missiles, and to detect an attack by weapons of mass destruction.

2. **The Medical Application**s:

With the development of science, medical field has been evolved. This type has many uses, as the cultivation of nodes in a patient's body to diagnosis a disease or to study the human body and monitor the patient's status. As appears in the figure (2.2) sensor nodes built in the human, and base station to control the work body to study the members of human body.

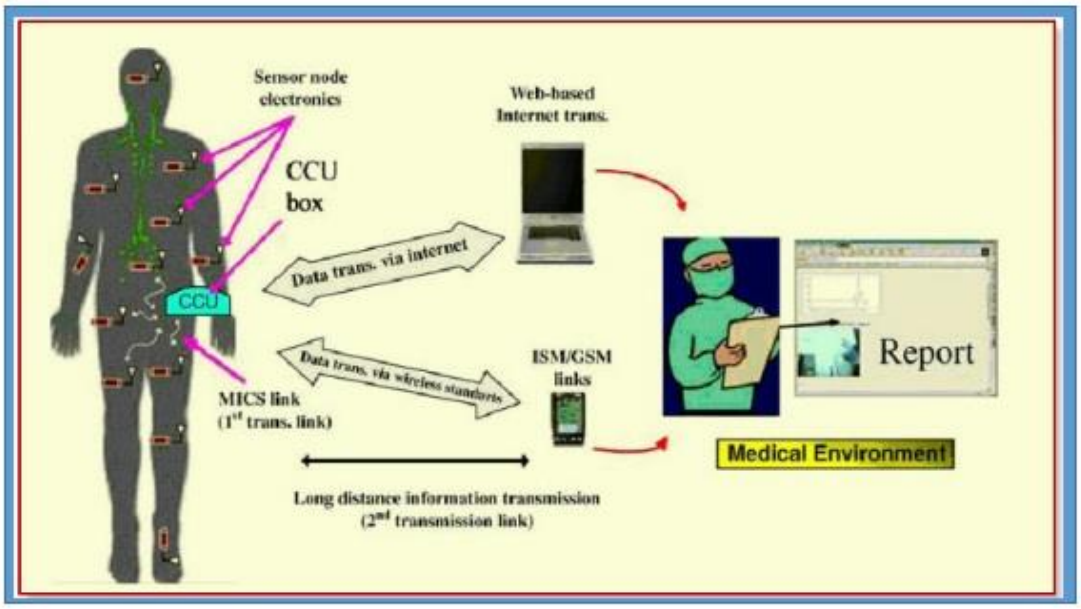


Figure (2.2) WSN in the medical environment [62]

3. **Industrial Applications:**

This application is included the industrial sensing and the diagnostics. Such as the appliances, the factory, and the equipping chains.

4. **The Infrastructure Protection Application:**

This application is included the power grids controlling and the water distribution controlling.

5. **The Other Applications**:

There are various applications in many fields such as in commercial industrial or whole service that make life easier to the humans and benefit from technology. The sensor nodes are built into home's devices (ovens, the fridge-freezers, and the electrical machine to remove dust and dirt). That is enabled them to interact with each other and it is remote in control.

2.7 Ad Hoc Networks:

It is a new technology in the networking world which is the first mobile networks without a fixed structure. It considers a self-configuring communication system. It used to use the nodes themselves as not only sources and sinks but also routers as appears in figure (2.3). There are several kinds of this network, such Mobile Ad Hoc Networks (MANET), Sensor Networks, and Vehicle Network. However, the basic rules of these wireless networks remain the same. But it has some variation. The effective use of resources is an essential to create high performance networks. This technology has a bright future in the communications field and a human service through its applications. The form of ad hoc networks consists of mobile nodes without any fixed infrastructure to nodes. Wireless communication is used to communicate the nodes together. Because of mobility nodes and the environment of nodes which are distributed, the probability for danger and lack of control is very high. The nature of these networks is attracted by many infiltrators and attackers, as a Gray Hole attack, Worm Hole attack, flooding attack, and Sybil attack. Sybil attack considers one of the malicious node that claims multiple identities. This attack is considered very dangerous to ad hoc networks [30] [25] [39].

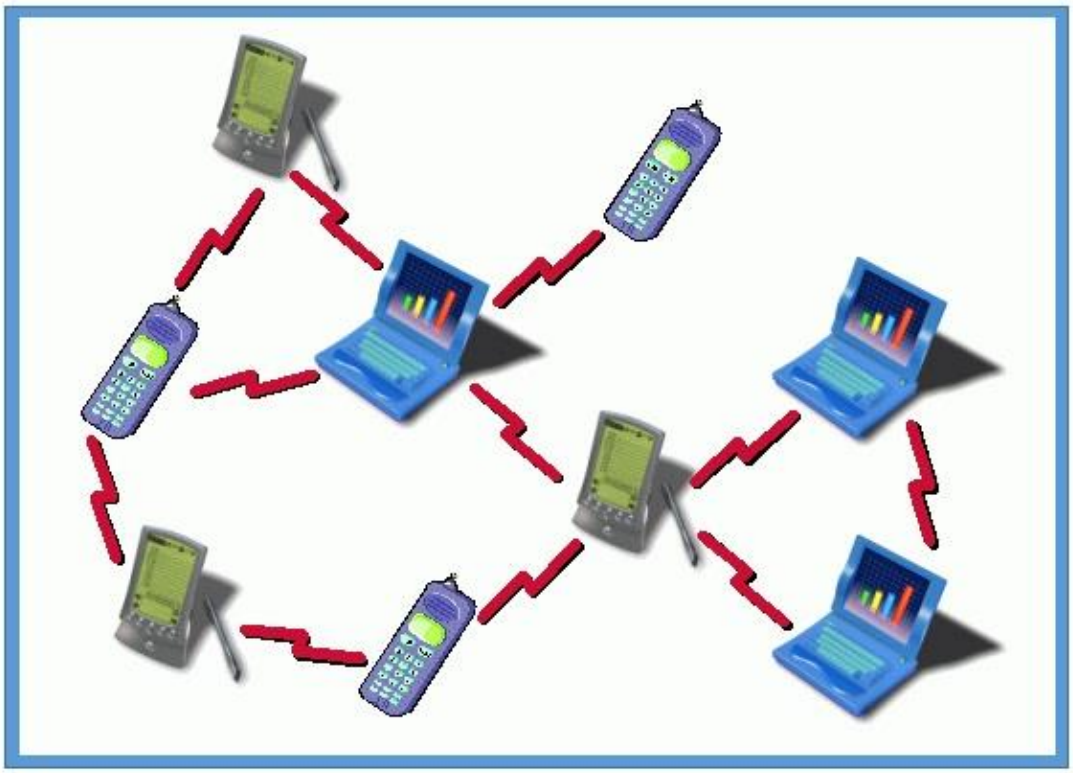


Figure (2.3) Ad hoc network each node as source and destination [39]

2.8 Application and Examples of Ad hoc Networks:

There are many useful applications in this networks such as [27]:

- **Military Tactical Operations**:

A communication network that depends on a fixed infrastructure is not practical for military tactical operations, as it represents a soft spot in hostile environments. Because it does not need to set up a fixed infrastructure that makes ad hoc networks perfect candidates for such operations.

- **Search and Rescue Missions**:

Some places as the top of a mountain, the middle of a forest or inside a cave could not use communication in the fixed infrastructure because that used to use ad hoc networks. It is easy to use communication systems for such scenarios.

- **Disaster relief:**

The ad hoc network provides the communication in an environment which its infrastructure is broken.

- **Law enforcement:**

This application can be extended to include locations with no communication infrastructure. Ad hoc networks systems provide fast and secure communication in this way.

- **Commercial use**:

Ad hoc networks can be used to support data exchange between people and applications in large meetings and conventions. Figure (2.4) and (2.5) shows some of these application.

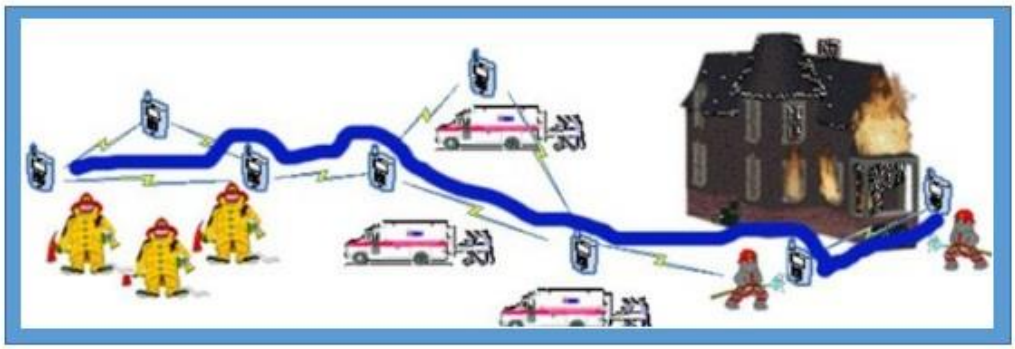


Figure (2.4) Ad hoc network in disaster [27]

Figure (2.5) Ad hoc network in the traffic monitoring [27]

2.9 The ad hoc Routing Protocols:

The nodes of this network behave such as a router and it find the safe route to other node. The protocols that are used in wired networks are not use in wireless networks. Varied protocols have been developed for this network. The classification of these protocols are the following [25] [28] [42]:

2.9.1 The Proactive (Table-driven) Routing Protocol:

It is also called table driven protocol. Each node has the routing table that is contain information about the network without requiring it. In this type of protocols, in periodically the mobile nodes transmit. The nodes need to preserve its routing table that is record the close nodes, the ready nodes, and the number of hops.

2.9.2 The Reactive (on-demand) Routing Protocol:

It is also called on demand routing protocol. This protocol discovers the path when it is needed. The nodes start to discover a route when it is requested. The reactive routing begins when the nodes wish to transmit the packets.

2.9.3 Hybrid Routing Protocol:

This type gathers the advantages of above protocols to overcome the weakness of them. It is use the route discovery technique of **reactive protocol**, and is use table maintenance technique of **proactive protocol** to avoid the latency and the overhead problems. A **hybrid protocol** is convenient to large network when the numbers of nodes present. The category of these protocols is shown below in Figure (4.4)

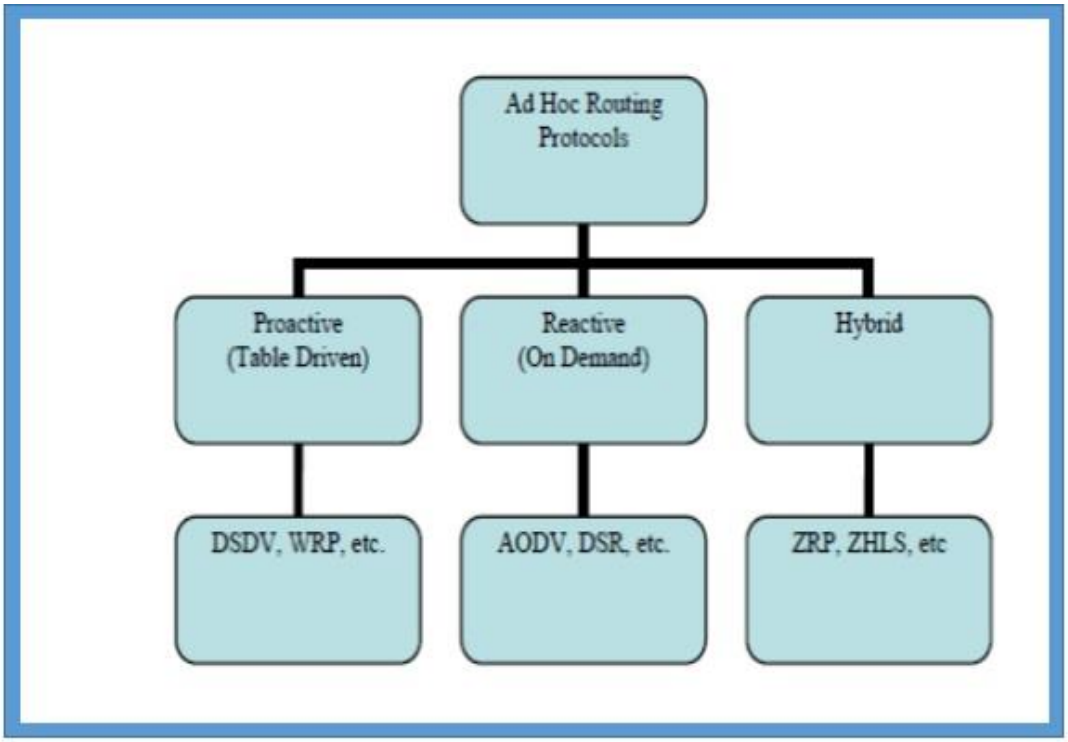


Figure (2.6) Ad hoc routing protocol [25]

2.10 Challenges in Ad Hoc:

There are many challenges in ad hoc networks as the follows. [28] [51] [4].

2.10.1 Routing: The structural of the networks works is without a fixed form. This makes the connection between the nodes (sender and receiver) difficult. The protocols that apply on this networks ad hoc network based on the principle of reaction rather than proactive. Another challenge is multicast because it is not static which causes the random moving of the nodes. The routes between nodes are contain multiple hops. That consider more complex than one hope.

2.10.2The Security and The Reliability:

Security is a major problem in ad hoc networks, due to losing the packets. There are different schemes of security such as the authentication, the key management, and the reliability problems. The limited of transmission range and transmission nature cause losing of packets and data transmission error.

2.10.3 The Quality of Services:

Several services in various environments create many challenges. The adaptation of QoS should implement in over classic of the resource reservation for backing the multiservice.

2.10.4 The Location Aided Routing:

The location aided routing uses position information to define the related regions. The routing is oriented and restricted. This is similar to the associative oriented and the restrict broadcast in ABR (Auditory Brainstem Response) [49].

Table (2.2) Comparison between (Ad hoc & WSN) [49]

Affected by	WSN	Ad hoc
The Efficiency of Energy	Bound battery size	Unbounded
The Network Size	Number of nodes large	Number of nodes little
The Density of Distributed	Depends on type of application	Depends on type of application
The Data fusion	bounded	unbounded
The Traffic Distribution	Rely on application	Rely on application

2.11 Security:

In these days the security considers the important challenges. The development of wireless technology makes the security measurement not convenient to wireless technology. Security wireless networks are responsible for prevention and authorization access to wireless networks and the damage of the computers. Wireless networks are most used in organizations and individuals. Nevertheless, wireless networking has many security issues that prevent attacks in the systems which are used to enforce the security policies. The wide use for wireless networks at the present time increases risks and attackers for these networks. Though of many security risks and attackers are prospered with wireless protocols and encryption methods. [10] [11].

2.12 Security Requirements: [10] [38]

Each company or system wants to protect its data from any danger, should provide a special and strong security system depending on the type of data. The security system must be complying with all the industrial, structural and operational system requirements.

- The essential condition is that the sensitive data is stored and transported through the wireless networks should be encrypted with approved algorithms.
- The requirements of using the authentication that is achieved by the USB dongle, security smart card [10].

2.13 Security Classes:

The classification of attacks as follows which appears in figure (2.7):

- **The Interruption:** an attack is cause the systems which are used become unusable, and the insertion of malicious code.
- **The Interception:** an attack is happened on confidentiality. The networks are cracked by the attacker to gain unauthorized access to the nodes.
- **The Modification:** an attack is happened on integrity. It is mean unauthorized part; it is not access to the data but change it. The modification of data being transmitted or causing a denial of services attack.
- **The Fabrication**: an attack is happened on authentication. It means false injection of data instead of the original data. Then, it sends the false injection to destination [12].

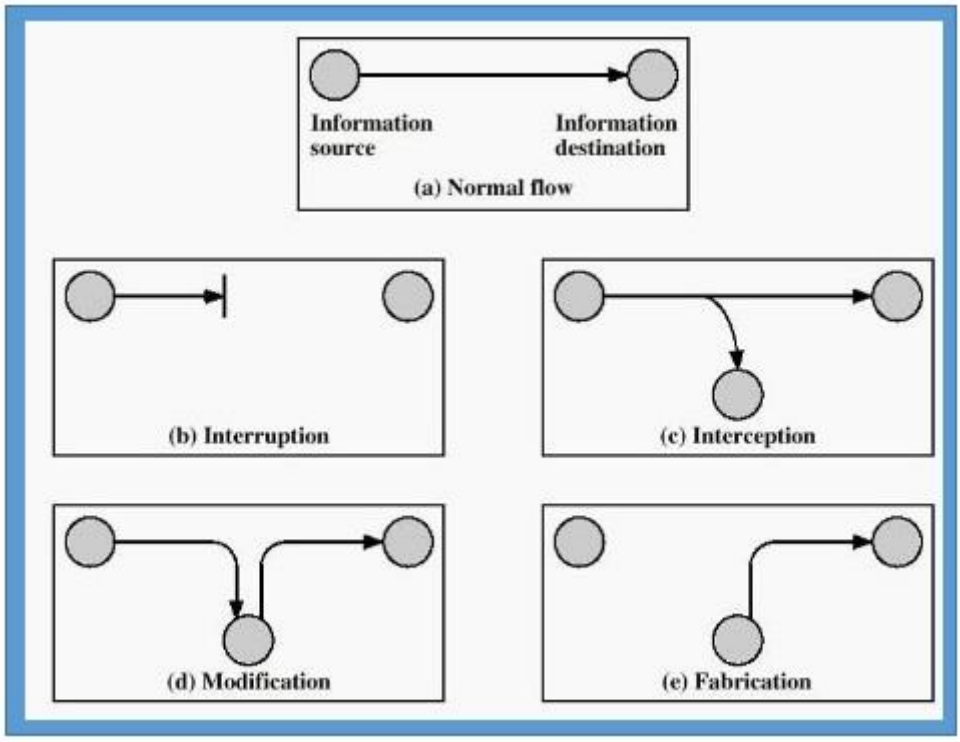


Figure (2.7) Classification of attacks [12]

2.14 Security Threats on Wireless Networks:

As appears in figure (2.8) there are many types of threats that affect on wireless networks. The protection of attacks can be providing by the confidentiality, the integrity and the availability. This section is explained the different types of security attack methods. These methods apply to break confidentiality and integrity, sometimes only confidentiality or only integrity. There various kinds of security are attacks shown in the following [10]:

1.The Traffic Analysis:

This method enables the attacker to access three types of information. **First,** the information is related to identification of activities. **Second,** the information that is important to the attacker it is identification and physical location of access point in its surroundings. Third, the information an attacker gets is by traffic analysis.

2.Denial of Service(DoS):

An attacker gets information before it reaches the required destination. It is cause wrong or misleading of information in the system. Sybil is considering one of denial of service attack. This intrusion is made by people not authorized to use other wireless devices to prevent authorized communication [13].

3.Brute Force Attack:

It is a passive attack that the attacker generates every possible in the key. Then it tries for decode the encoded message which is generated alteration with validates output [15].

4.Placement of Message Integrity Check bits:

This type of attack considers a problem because it uses by a hacker with the validate contents. Then it decrypted the message [10].

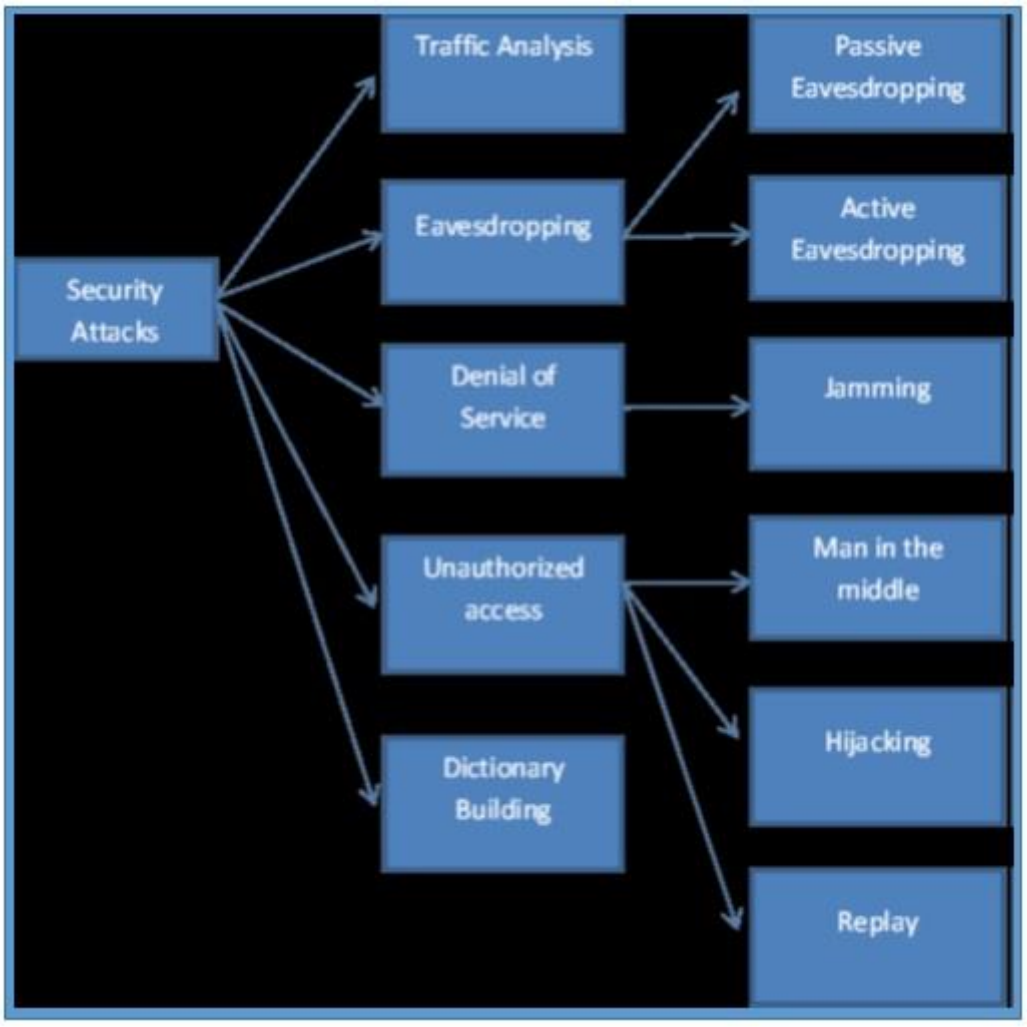


Figure (2.8) Threats to wireless networks [10]

2.15 The Sybil Attack:

In the first time, in peer to peer networks there Sybil attack was found. It creates multiple identities from one node. It illusions the normal nodes through the multiple identities. Sybil node is illusion to the nodes in the network traffic is very heavy near him, that leads the traffic following him choose alternate route. After that Sybil attack it gets empty route to himself. In Sybil attack one malicious node have control over other Sybil nodes. Then it has control over all the networking protocols. The obtaining of a new inexpensive identity encourages Sybil attack to create itself in Ad hoc and WSN. Sybil node create several virtual nodes by simply assuming a new identity [5]. As what happened in 2014, it is exposed NSA/CIA by Sybil attack then it was exposure to large financial loss. Sybil attack considers very dangerous to wireless networks because it considers the entrance of different attacks. This type of attack causes damages in divided storage, in voting, and in resource allocation. It is appeared in ad hoc &WSN. There are many methods to protect the wireless networks. As shown in figure (2.9) Sybil attack and how it locates between normal nodes [5] [16] [17].

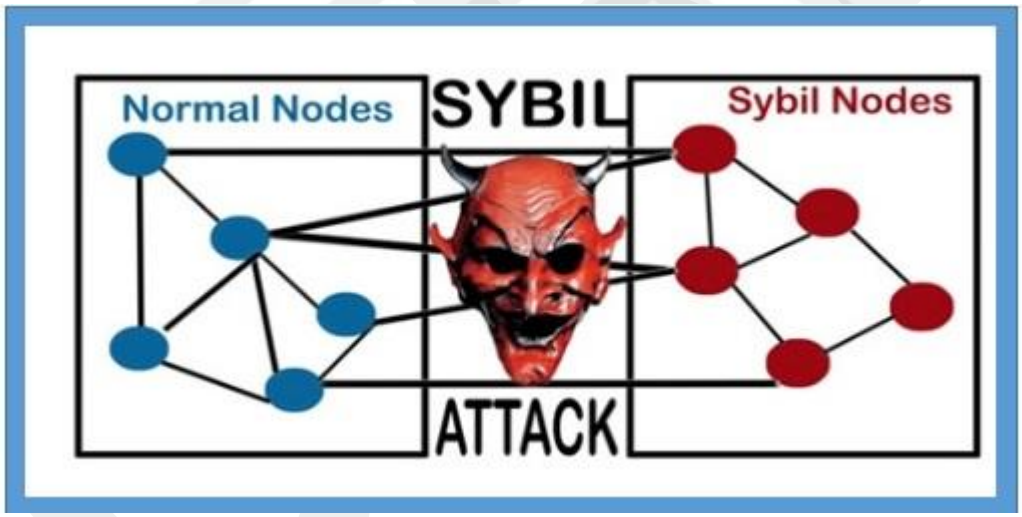


Figure (2.9) Sybil attack [5]

2.15.1 Creation of Sybil Nodes in Wireless network:

To creates Sybil attack in wireless network there are several ways based on the communication, simultaneity and fabricated identities. It depends on how the nodes communicate with normal node. Then it gets the information from the normal node like the position and the ids. Sybil attack uses this parameter to create the same type of identities then Sybil attack will destroy the network [16] [18].

1. **Direct and indirect communication:**

   The Direct communication: when a node (Sybil) is communicated to a normal node directly.

   Indirect communication: when a node (Sybil) is not communicated directly with normal node but by malicious nodes it is connected by intermediate node [12].

2. **Stolen and Fabricated identities**:

   The Fabricated identities: it deals with the creation a new identity by the attacker.

   The Stolen identities: it deals with stolen identities of a normal node by the attacker. It creates a new identity similar to stolen identities.

3. **Simultaneous and no simultaneous**:

   The Simultaneous: it creates multiple identities which participate in the network at same time.

   No simultaneous: it creates identities which participate in individual time.

2.15.2 The Types of Sybil attack:

Depending on the network behavior there are many types of Sybil attack. As the voting, the distributed storage, the data aggregation, the resource allocation, and the misbehavior detection.

1. **The Distributed storage:**

In this type, Sybil attack goes on the data replication and the data fragmentation. The first type means the uniformity between the excess resources by sharing information.it is attack to same data that is stored in multiple storages. The second type is same the processing tasks execute in many times. The attacker listens to the same account of tasks, that broadcast the identity then it gets the data from memory easily [16] [17].

2. **The Routing:**

Sybil attack forgeries the number of nodes with multiple identities. However, it uses the multiple paths in a network. It attacks the geographical routing protocol and location based on routing protocol because the multipath routing. The node exchanges the location information between the nodes. Then it addresses the packets geographically during this routing. Each node is send the packet to the suspicious node and then Sybil node does not transmit the packet to correct node [16] [17].

3. **The Data Summarization:**

It is a tool to reduce a communication cost of saved energy and it is easy to avoid the redundancy of data. The data summarization is costumed to summarize the result by using queries in different regions. Then it passes information from one node to another [16] [17].

4. **The Voting:**

In some wireless networks the decisions are made by the voting. Sybil attack has several identities, one node has chance for voting many times, consequently destructing the process [16] [17].

CHAPTER 3

Literature Review

Detect and Prevent Sybil Attack in (WSN and Ad hoc)

3.1 Introduction

Many efforts have been made and several security models have been proposed for identify and avoiding Sybil attack. Most of proposed methods are able to detect Sybil attack but some of these mechanisms are limited or impractical to apply it. This chapter discusses some of these models and mechanisms which have been proposed to identify and avoid Sybil attack in (Ad hoc and WSN) networks.

3.2 Detecting Sybil Attacks in Ad Hoc Networks:

The broadcast nature in transmission medium and an architecture of ad hoc networks make several attacks to penetration the networks especially the Sybil attack as it was defined in chapter two. For this reason, many researchers have made several studies to detect and prevent Sybil attack. The following summary of these studies depend on the name of the researcher.

3.2.1 Douceur in [44]:

This study explained the resource testing scheme to prevent Sybil attack in ad hoc networks. This algorithm is based on the assumption. There is a limited resource for each physical entity. So, depending on this scheme computation, storage, and communication can be used for resource testing. The scheme of this method assumes each node has just one radio which does not capable of send or receive on two channel simultaneously. If a node wants to check the presence of Sybil nodes with its neighbors, it assigns its neighbor's in different channel to broadcast the messages to a node. Then it is select randomly a channel to listen. The node hears a message on the channel that is assigned by the verifying node. it considers a normal node else the neighbor's node is treated as the Sybil node.

Problem

- Firstly, how the sensor node assigns a radio channels to their neighbor nodes.
- Secondly, this algorithm is consuming a large of battery power.

3.2.2 Zhang et al. in [45]:

Another algorithm has introduced the concept of location-based cryptographic keys, called pairing. In this algorithm, the private key of each node is added with its ID and the geographic location. The Location Based Keys (LBKs) are generated pairing that based on identity of cryptography by an authorized person. This method includes a secure LBK based neighborhood authentication and the ways to establish both the immediate and the multihop pair wise that is shared keys. If Sybil node wants to take a legitimate node and does not have the authentic LBK it cannot finish mutual authentication with other normal nodes in successful manner. Sybil attack cannot claim false IDs and locations without discovery. Then, the Sybil attack is detected in an effective way.

Problem:

- This algorithm does not work in large ad hoc networks.
- The pairing consumes an energy.

3.2.3Arpita M. Bhise et al. in [47]:

This scheme is based on a behavior of packet that are entered to a network. Sybil node creates fake identities that is deceive the system. Then it controls of a network (denial of service (DoS)). So, the proposed method is also based on this behavior. It is work on behavior of received packets. The incoming packet is a carrier its identity and its location where to place. The IDs and locations is help to distinguish between the normal packets and Sybil packets. When (IDs and locations) of the packet is entered, it is same the received packet. Then it considers as the legitimate packet. But if the incoming packets copies that creates the fake identities in different location and it is detect Sybil packet.

Problem:

This method required for knowing ids and location to determine attack. This process needs a long time to check the ids and location.

3.2.4 Piro et al. in [24]:

This algorithm uses the mobility of nodes as a feature to detect the Sybil attack in ad hoc networks. This mechanism considers all the Sybil nodes move together. If sets of nodes are seen together for a long period of time by a monitor node, then they are suspected to be the Sybil node. When using multiple observer nodes, the accuracy of this algorithm increases.

Problem:

- This algorithm will be fails if the Sybil node continuously changes the identities of its.
- The legitimate nodes can also be forgery by the Sybil attacker.

3.2.5 Bazzi et al. [46]:

This approach is proposed Sybil attack is based on network coordinates in order to differentiate between nodes. The mechanism in this algorithm is based on assumptions. Sybil attack have only one position in network that is defined in terms of its minimum latency to a set of beacons. If the node is want to authenticate itself, it presents a geometric certificate. That consists of verified ping times and a set of standardized beacon nodes. The multi virtual machines is located at the same physical location with the same certificate is address as one node.

Problem:

- If there are N malicious nodes with d different network positions thus, break the protection of this method.
- The method very complex and energy consumptive.

3.2.6 Newsome et al. also in [47]:

This method is proposed the random key pre-distribution and registration. It is based on key validation; in this model each node is choose keys in randomly from the pool of' keys. The pool selects two nodes that share one key with some probability. The identity of the nodes is combined with set of keys. So, all nodes are authenticated by verifying some or all keys that it is request to possess.

Problem:

- This method requires more memory space for storing pair wise keys with its neighbors.

- Secondly, if an adversary is somehow able to compromise some keys.

  it falsely requests the identities of several non-compromised nodes.

3.2.7 Diogo M´onica [6]:

The author in this thesis used the Byzantine fault-tolerance techniques to prevent Sybil attack in ad hoc network secure that typically depended on quorum based security protocols. However, this protocol is possible to lose easily if one element partnered with multiple identities in the network.

Problem:

The proposed method allows the normal nodes in one hop neighborhood to have set of non-Sybil identities. The combination of many types of resource test is rely on this method.

3.3 Protection (Measurements) Sybil Attack in WSNs:

The protection of WSNs is the most important part. The Security in WSNs are complicated because the broadcast nature of the wireless communication and there are does not have hardware for the protection. The Sybil attack is a massive destructive attack to WSN as was described in chapter two. There are many algorithms to prevent Sybil attacks. Each algorithm has advantage and disadvantage depends on how works this algorithm and its environment. The most important thing to prevent Sybil attack, it knows how the attack creates itself. The following algorithms was proposed by different researchers to prevent Sybil attack. It summaries according to the name of the algorithms:

3.3.1 Random Password Comparison to Prevent Sybil Attack:

This algorithm is proposed to address the different traffic levels and security considerations during the data transmission in a WSN. Assumes the network G has a base station BS, and comprises of N number of nodes deploys randomly. This algorithm contains the routing table (R table-RPC) to store the information's nodes (ID, time and password). The intermediate nodes in route are identify between source and destination nodes. Then it compares with RPC database. The information if matches, the node considers a normal node otherwise node considers Sybil attack [55].

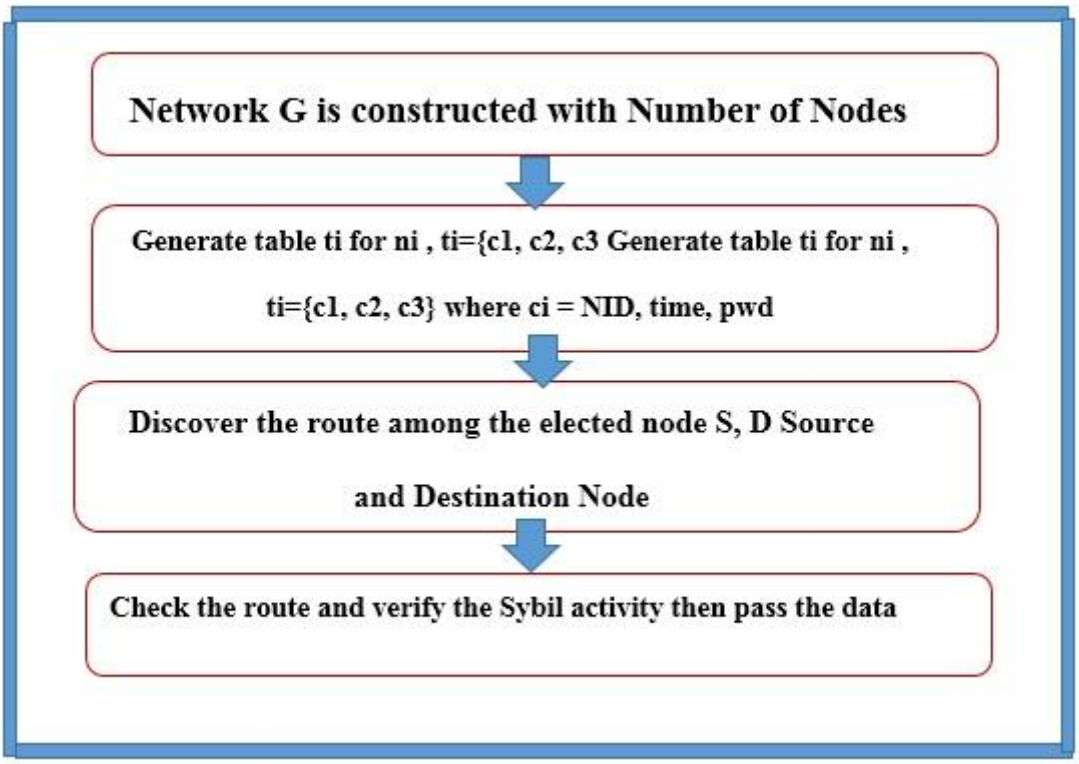


Figure (3.1) System model of random password comparison [55]

Problem:

- It is necessary to include the route repair mechanism, in case of route failure.
- The table-RPC is increased for more number of nodes that is distributed in the network.

3.3.2 Based on RSSI:

The RSSI is the received signal strength in a wireless. This method is based on getting a position of nodes and on signal strength. Each node has the same power and computing capability. The positions of nodes consider fixed. The network considers safe when the nodes use the signal strength [24] [56].

Problem: There is one drawback, is the nodes are time varying.

3.3.3 Ant Colony Based Sybil Detection:

This proposed assumes a protocol to limit the influence of Sybil attack by combining ant colony optimization (ACO) algorithm, on ant colony optimization (ACO) algorithm. When the node is move randomly it leaves traces on the path. It is based on the nature of the ACO and limit number of attack. The system ensures a normal node that is accept. The normal node accepts with high probability and Sybil attack rejects with less probability in the network [57].

3 .3.4 Using Sequential Analysis to Detect Sybil Attack:

This method works in two stages. First, it collects the evidences by observed neighboring node activities. Further, it collects evidences that are consolidated to provide input to the second stage. In the second stage, collects evidences that are validated using the sequential probability ratio test to decide whether the neighbor node is Sybil or benign [58].

Problem: it is take a long time to assign penetration

Chapter 4

System Model of Proposed Method

4.1 Introduction of Vehicular Network:

Vehicular networks are particular kind of mobile ad hoc network (MANET). In this network used to use vehicle nodes. Vehicular networks have some limitation such as quickly change in topology, not power bonds, large-scale, change of the network density and aloft predictable. Usually the vehicles are moving with finite speed in the road with a constant configuration of the road [59]. VANET is designed for increasing comfortable ride, control vehicle traffic and road safety. For example, vehicles cooperate with us for sensing information about traffic jams and send to the rest of the vehicles, or to the Department of Motor Vehicle (DMV) to facilitate traffic rerouting. As appears in figure (4.1) VANT.

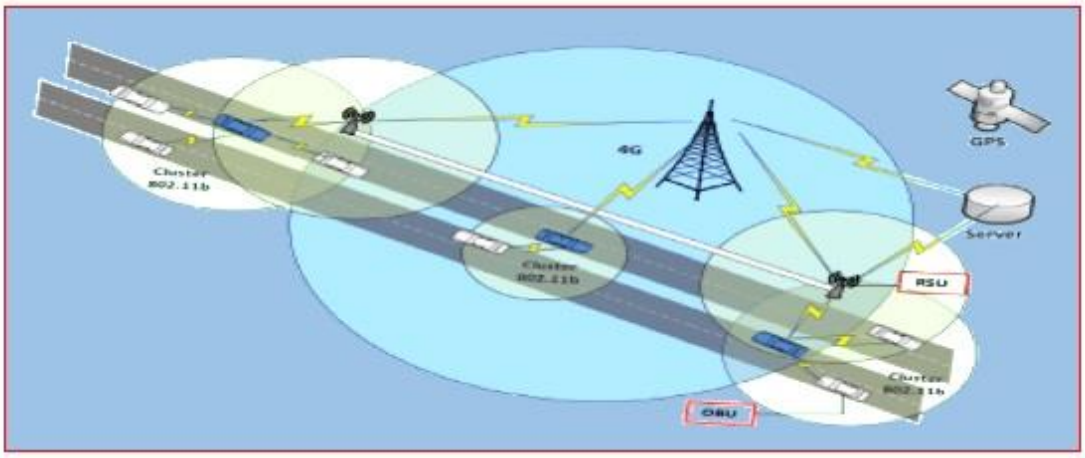


Figure (4.1) Vehicle network [59]

The comminution between vehicles in VANTs occurs through:

1. The Vehicle to the Vehicle (V2V).
2. The Vehicle to (RSU) and OBU (V2I).

The second type of communication it means the vehicle connect to the infrastructure with 2 communication devices called the Road Side Unit(RSU) which is placed on road side and On Board Unit(OBU) that is installed in vehicles. VANT is need to sensors that is installed on vehicles to collect environmental and road information [60] [61]. The medium use to communicate amongst vehicles is 5.9 GHz. There are many attacks vulnerable to wireless networks. Sybil attack considers one of important attacks that was described in chapter two on this thesis [31]. There are many operations of Sybil attack in various environments to destroy networks. This chapter presents the proposed

method to detect and prevent Sybil attack. It is based on base station to forward all the information about nodes to the Department of Motor Vehicle (DMV),then it allows DMV to check the autographs of all messages. The main purpose of the thesis is to detection and prevention of Sybil attack.

4.2 The Structure of Proposed Method:

This section illustrates the structure of the proposed method to detect and prevent Sybil attack. It is assumed all nodes communicate in multiple hop manner. The Road Side Box(RSB) is connected to the Department of Motor Vehicle(DMV) by the wired network. DMV is responsible for certificate authority (CA) and manage vehicle registration. The proposed method is based on DMV that provides a **pool of keys**. Each node takes its key from the pool. These keys use to hide the node's information. The assigned key is hashed to a specific value, the hashing value used to prevent a node from using **multiple keys**. By calculating the hashed values of keys to RSB and DMV to determine if the keys are come from same pool. In this way the detection of Sybil attack is happened.

4.2.1 The Department of Motor Vehicle (DMV) :

This considers authenticate part that saves the node record and distributes keys to each node.DMV has sufficient resources for producing the keys in quickly manner.Then is store all the information about the nodes. It is responsible for any authoritative certificate.

4.2.2 Vehicles:

There are untrusted parts.The communication between two of the nodes in multihop manner. The messages is exchanged between two nodes is signed by DMV.

4.2.3 Road Side Box (RSB):

RSB is like wireless access point. It is put along the roads and linked to DMV by wired network.It works as intermediate node to DMV. The RSB observe nodes activity and it is identify the suspicious behavior then it makes a report to DMV for confirmation. Sometimes DMV is may be attacked, for this reason it cannot be used for critical functions. Nevertheless they, it improves the scalability of the network. The proposed method can display as figure (4.2).

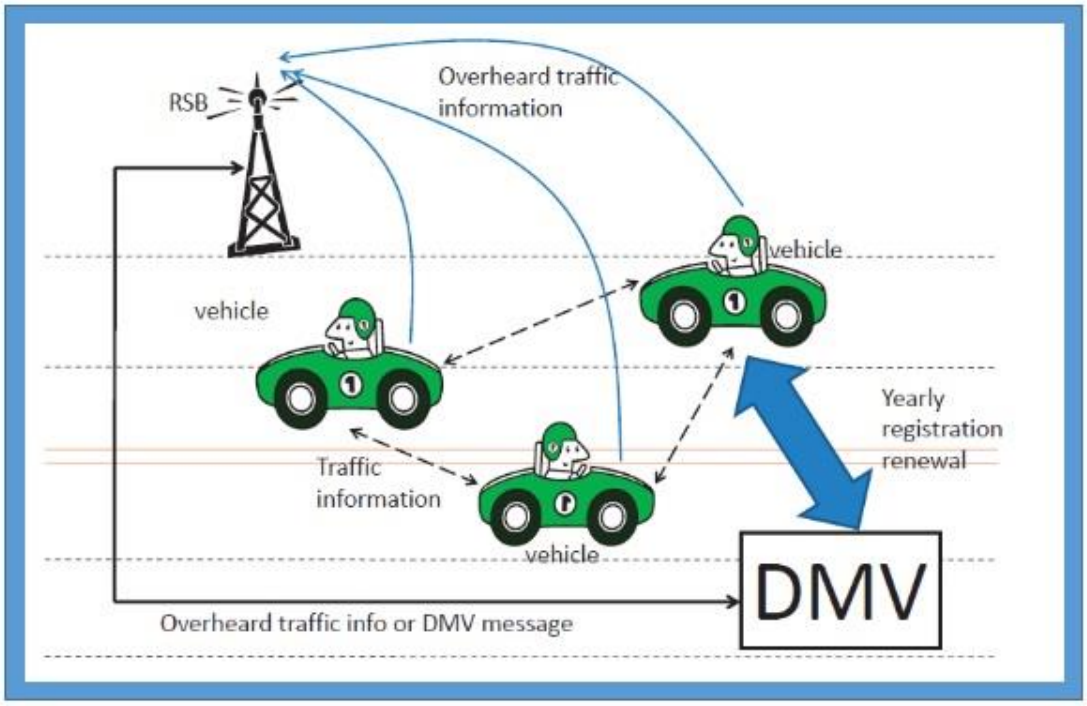


Figure (4.2) The architecture of the propsoed method

4.3 Attackers Actions in The Proposed Method:

This part explains the actions of attackers which are expected to occur in the propsed network, as the folowing:

4.3.1 Advertise a False Message and Inject False Data:

The nodes sign a false message then it is broadcast to other nodes.The message cannot recognize the attakers because it is signed by a CA.This attack can have an effect on a voting system, the voting system fails if the attacker generates enough false identities to break the normal vehicles.

4.3.2 Sybil Attack*:*

A node is consider Sybil attack when it uses multiple keys to sign one message. The node specifies from a set of keys that can use.In this point the privacy of node is compromise. The nodes and RSB hear multiple messages that is signed by attacker. They cannot recognize these keys if it belongs to the same node.

4.3.3 Compromised to RSB*:*

RSB are Semi-reliable part. The RSB is compromised by the attackers. If the RSB is compromised,it is easily detected by the DMV. Then it is removed quickly. So , the attackers can gain information that is stored in the RSB.

4.4 The Structure of Event to Sign the Message :

In VANT the nodes broadcast a special events to sign the message then it control them. Must to find the sum of nodes that are send the same message.

The event is a row of information ,it is set as **(t, l, e)**. It creates predefined time (**t∈T)** in predefined area (**l∈L)** for type of event(**e∈E).** The **(T-L-E)** are dyployment to each node in the VANT. As is explained in chapter 2 ,Sybil attack is exploite the VANT with multiple keys.The event is prevent the attack through the limitation of using the keys,it means **a normal node uses one key that sign one event**.To recognize normal use from wrong use of keys through the following , if one node uses two or more keys to sign one event , as two or more nodes are report the same event. This action considers **Sybil attack.**

4.5 The Proposed Method Scheme:

In the proposed method DMV is responsible for detecting attacks with the help of RSB. RSB talks DMV when is suspected malicious node that is need to confirm. The RSB are not reliable part because that, the nodes information is available to DMV cannot transfer to RSB. There several constraints of the proposed method, because that the nodes are divided into groups then it releases the group information to RSB. This information is allowing RSB to detect a suspicious behavior. This information is not enough to RSB to track the equivocal nodes because of RSB does not distinguish between a node or a group of nodes. The creation a group of nodes is used by one-way hash function, that hashes the keys through the initialization step.

4.6 The Initialization Step:

- Firstly, DMV knows the total number of nodes it is register each node.
- DMV is responsible for generating enough yearly keys for all nodes.
- After producing the keys that assumes is **p:**

a) DMV first is hashed **(p | κc)** by using a one-way hash function, when **κc** is consider a global key.

b) Then DMV selects the set of bits for that is hashed. The selected bits are named as "**coarse-grained hash value**".

c) After that, the key **p** is placed into a group that is store the keys with the same coarse-grained hash values.

The other format, each key **p** in the S-th coarse-grained group, have **H(p|κc) = Γm** wherever **H** is consider a one way hash function, and **Γm** is consider the coarse-grained hash value for group **S**. These groups are named as "coarse-grained groups".

- **Next,** DMV is calculate the hash value for above **p** with a new key **κf** .
- DMV is select the set of bits for the result.This selected bits are named as the "**fine-grained hash value**".The key **p** is put into a subgroup of the coarse-grained group, is named **fine-grained group**. All the keys have the same **fine- grained hash value**. Each key **p'** in the ***R*-th fine-grained group** under the ***S*-th** coarse-grained group, it have **H(p' |κf) = Θn** where **Θn** is consider as the **fine-grained hash value** for the subgroup ***N***.

The above steps are named as "**two level hash**". As appeares in the figure (4.2). DMV holds the generating and the two level hashing keys until all finegrained groups hold a sufficient keys for a node's use.Then DMV is load a unique finegrained group of keys to each node at the time of yearly node registration.DMV is store the corresponding **(Γm|Θn)** as the node's secure plate number. Through the above details DMV is show the map from secure plate numbers to nodes is one2one. Consequently , DMV is must careful when it selects the length of **(Γ*m* &Θ*n)***.The secure plate numbers must be greater than or equal to number of nodes.

The two level hashing is keep storage to DMV because DMV is link a key to a node by computing its **coarse-grained** and **fine-grained** values. Thereafter, DMV is compare them with the secure plate number **(Γ*m*|Θ*n*)**. This process is avoid for needing the preserving node secure plate numbers and key collectivities. After the initialization stage DMV is keep the secure plate number for each node and the finegrained hash is key **κf** .In the figure (4.3) shows the DMV.

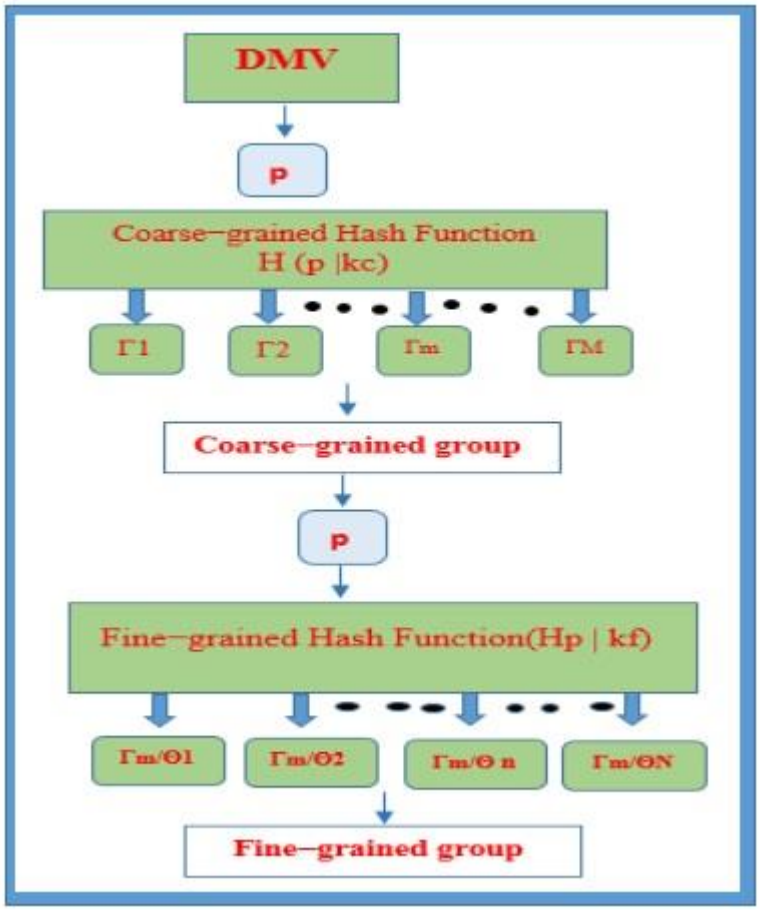


Figure (4.3) Work of the DMV

4.7 Generating the Keys:

The lifetime of coarse grained key **κc** takes into account when it produced the keys. Sybil attack can access the RSB and can know the keys for all nodes in this time. The privacy of nodes are based on the lifetime if it is too long the privacy is considered bad. Thus , the keys must give short lifetimes such as two days or less.The initialization stage is divided the time into Q intervals and each interval is one day.

4.7.1 The Initial key Generation:

- DMV uses a series of coarse-grained keys **Kc** instead of one key, **κc** to hash the keys.
- Each key **κc,R ∈ Kc** is generate keys for the **R**-the time interval.
- The keys that are hashed to **Γm** with the key **κc, R**. It is placed into the **S**-th coarse-grained group and it can use in the **R**-th time.
- When the time is finished the keys are rejected.

4.7.2 The Expired Keys:

This subsection is explained the advantage of the proposed method to prevent Sybil attack. The expired keys use to sign the events. DMV uses the various keys to generate certificates for keys in various time .The nodes is distinguish an expired key by check thire certificate.As the folowing steps how to create expired keys.

- DMV keeps all the coarse-grained hash keys at the beginning of **R**-th time.
- DMV sends the key **κc,R** to RSB.
- RSB keeps each valid coarse-grained key just for short time.
- If RSB compromises, Sybil attack gains just the coarse-grained hash key for the present time .
- The limitation of fine-graind key **kf** can not be assumed because of DMV cannot release it .
- Sybil attack cannot gain fine-grained key **kf** by compromising RSB .

4.8 Detection of Sybil Attack :

The basic idea of the proposed method is for detecting Sybil attack. RSB hears all the nodes with its communication range when the nodes communicate with each other. RSB put the keys that are used to sign the event **(ti- lj-ek)** in the list **(Li-j-k**). When all keys are collected to event **(ti- lj-ek)**. To detect Sybil attack in RSB will be as the following :

1. RSB passes each key **p** in the list (**Li-j-k**), and it is calculate the coarse-grained hash value **H(p|κc).** (Remind: the **κc** before is deployment to RSB in the initialization step.)
2. Subsequently it compare:

$$\text{If } \exists p, p' \in Li,j,k \text{ such that } H(p|\kappa c) = H(p'|\kappa c)$$

3. RSB observes two keys of the same coarse-grained hash value that are used to sign event **(ti- lj- ek)** as the following:

(a) **Sybil attack** is one node when use multiple keys to notify the same event.

(b) **false alarm** is an event notify by two nodes that keys are in the same coarse grained group.

RSB does not distinguish between (a) and (b). RSB is send a report to DMV which is contain :

1. Event **(ti- lj- ek)** .
2. The hash value is **Γ**.

3. The keys that coarse-grained hash value is **Γ**.
4. The signatures of the event.
5. The certificate of the keys.

When the report is received by DMV, it is checked for the signatures and the coarse - grained hash value **Γ** to prevent a compromised RSB .If RSB fixes to be authentic, DMV computes the fine-grained hash value **H(p|kf)** for each key **p** in RSB report.

If $\exists p, p'$ in the report such that $H(p|\kappa f) = H(p'|\kappa f)$

DMV is consider **p** and **p'** are from same node that is **Sybil attack**.Then, DMV is take moreover action to remove Sybil attack. This approche guarantes to detect Sybil attack.

4.9 Remove the Keys:

When a Sybil attack is detected ,DMV must remove all the keys. This part explains three possible methods to remove the keys. To select one of these methods it is based on the resources of the network. The summaries of these methods has the following:

4.9.1 Revocation of theTamper Proof Device (RTPD):

This type requests to hardware instaled on the nodes. In a Tamper Proof Device (TPD) used to store keys and to sign messages that are installed on all nodes. When is observe Sybil attack, DMV is send a removing message to the TPD. Then the TPD is erase all the keys and it is stop the signing messages. In this method DMV removes a node in one message.

4.9.2 Revocation Using Compressed Certificate Revocation Lists(RC2RL)

This method does not use hardware as TPD. It creates a **bloom filter(BF)** for all the keys to be removed. The bloom filter broadcasts to all the nodes. When a massage is received the node is use the BF to check its key. Then it drops, if the key is found removed,the capacity of all FBs is detected such as 10s of Kbytes. DMV needs to flood tens of Kbytes to remove a node during the network.

4.9.3 Create Secret Key to nodes"Backdoor":

The last method creates a secret key to the nodes. These key considerers such a “backdoor”. The Group Signature(GS) scheme that proposed in [54] is used to produce as a backdoor. In the GS approach, all nodes are balanced between group public key **gpkCA** and private signature key **gskV** .Then, it generates its own keys.

Chapter 5
Simulation and Result

5.1 Network Simulator by NS2:

NS2 is an open source simulator. It was designed to research in computer telecommunication networks. From 1989 until these days NS2 has great desire by industry, academia, and government. After many years of researching and development NS2 contain the modules for numerous network components that are as the routing, transport layer protocol, and application. The examination of network performance, the researchers are use the scripting language for configuring the networks, and monitor the results.NS2 is widely used in the open source network simulators. Figure (5.1) shows the scheme of NS2 program [42] [43].

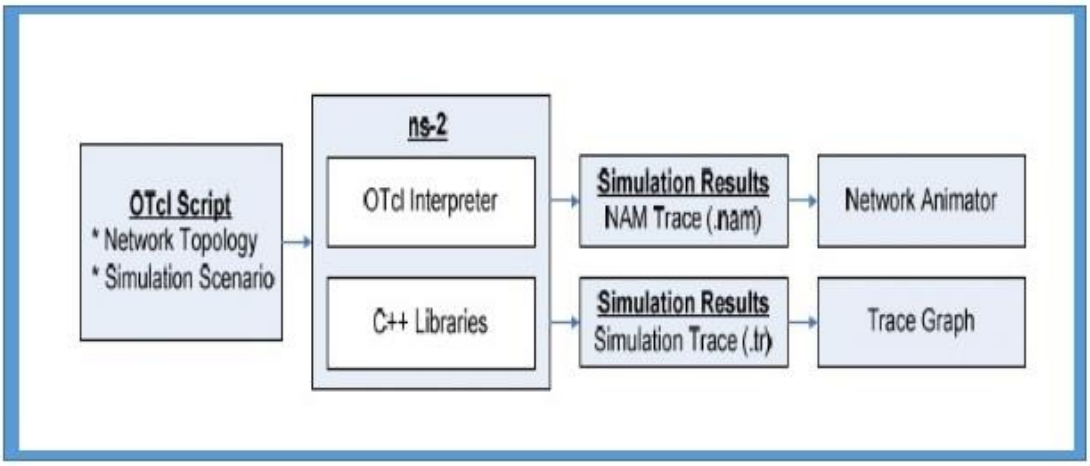


Figure (5.1) NS-2 schematically [42]

The core of NS2 is written in C++, and it is available for different platforms. However, users interact with NS2 via writing TCL (Tool Command Language) scripts. It must contain all of the commands needed to run the simulation such as setting up the topology, specifying and wireless parameters, etc. There are several simulators such as Riverbed Modeler Academic, OPNET Modeler, Matlap, and OMNeT++ [42],[43]. Table (5.1) shows the comparison between four simulators based on different factors.

Table (5.1) Comparison between simulators [43]

Factor	Opnet	QualNet	Ns-2	OMNet
Topology definition Language /Model	Proto-C.OO models	Parse ,C	C++ and OTcl	Flat files C++
Input/output definition	GUI based editor ,Proto -C	Flat files	OTcl based files	Flat files
OSI Layers	Available	Available	Available	Basic modules
Radio propagation Models	Available	Unknown	Available	Not available
Traffic generation	Available	Unknown	Available	Not available
Modifiability	Moderate	Not so easy	Complex	Good
Licensing	Commercial	Free for universities	Public domain	Public domain
Scientific acceptance	Reasonable	Good	Very good	Reasonable

5.2 Simulation Setup :

The proposed method is simulated by NS2 .The Secure Hash Algorithm1(SHA-1) is used as hash function.SHA-1 is special category of hash function which have certain properties that makes it appropriate for using in cryptography.SHA-1mathematical algorithm which maps the data of arbitrary size to the bit string of the constant size (a hash function).It is designed as one way function ,it is not possible for inverting. Often input data is named message**,** and output (hash value or hash) is named the message digest or simply the digest. In figure (5.2) shows the work of SHA-1.

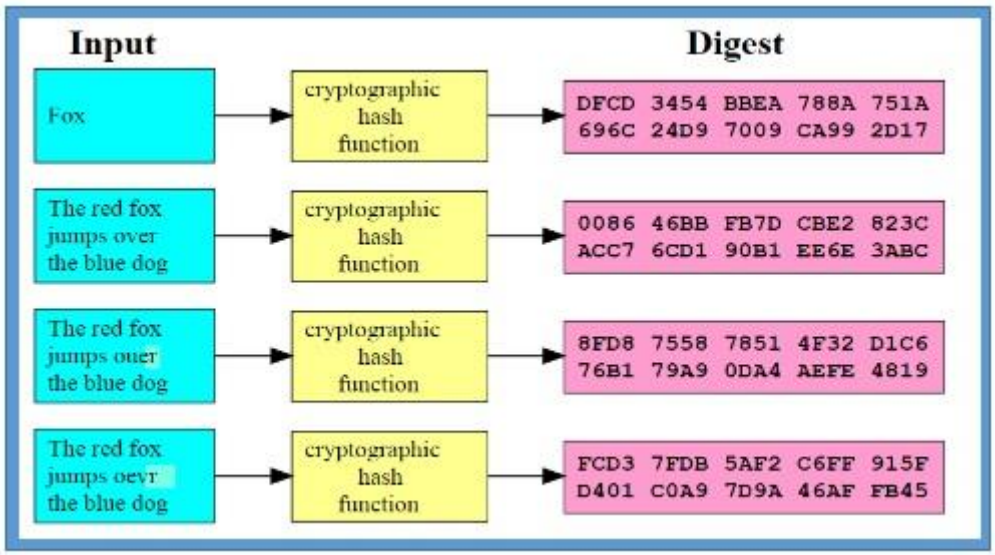


Figure (5.2) SHA-1 Secure Hash Algorithm 1 [63]

- In the first step of the proposed method in the initialization stage, is used SHA-1hashing function for producing keys that are sufficient for using.
- The major simulation parameters are shown in table (5.2) .

Table (5.2) The Parameters of Simulation

Parameters	Value
The length of street(m)	2000
The communication of radius(m)	300
The width of street	4
The width of path(m)	4
The speed of vehicles (m/s)	30-40
The keys on the day	20
The packet rate (pkts/s)	3
the time of work(s)	400

- In this simulation it is generated randomly events with various **(time-locations- types)** , then is stored them in an array.
- When generated events, it is assumed length of time= 20 seconds. The length of location = 250m. The total number of 5 the event types.
- Every node can access in periodically manner to array, it gains events with the present time and the location node, and it broadcasts them.

There are four types of nodes:

A. Normal node
B. Malicious node (Sybil attack)
C. RSB
D. DMV

The normal node is sense periodically the events, and sign then it broadcast them. Sybil attack produces the random number of the events. Thereafter it is sign every event with multiple keys and it is broadcast them. The RSB, DMV their works have been mentioned in the previous chapter.

5.3 Generating Keys in Theoretical and Experimental :

This section presents the result of simulation for the proposed method to detect Sybil attack**.** It is supposed **NV** nodes in total and each node is need **M** keys. Also it is supposed a hash function producing equally to distribute hash values.

- **Firstly**,it is calculate an upper limit that is expect of number of keys means DMV is find for all nodes.
- It begins from **M = 1**.,The expected number of generated keys is :

$$Np \equiv NV \log NV + \mu NV + 1/2 + o(1)$$

$$\text{where } \mu \approx 0.577.$$

$$\text{for } M > 1$$

$$Nu = M \times (NV \log NV + \mu NV + 1/2 + o(1)).$$

Furthermore, it is found the definition of **Np** that it have the lower limit **O(MNV)**. Then, it is concluded that in order for generating year's keys. The number of keys which DMV is need for generating is between **O(MNV)** and **O(MNV logNV)**.

- **Secondly** ,it is calculated the cost of generate keys. In this scheme ,the keys of all node are divide into **d** equal divisions. All divisions are mixed of special key. DMV is needed for generating **M/d** keys for each node with each hash. So, it has:

$$Nu = d((M/d) \times (NV \log NV + \mu NV + 1/2 + o(1))) \quad (1)$$

$$= M \times (NV \log NV + \mu NV + 1/2 + o(1)) \quad (2)$$

The **lower limit** of number of keys stills **O (MNV).** Then, the **upper limit** and the **lower limit** of the expected number of generated keys residue the same. So, each time has only one key, the expected number of generated keys reaches the upper limited Nu.

- Then, it is used the simulator NS2 to generate the keys. In the figure (5.3) compare between theoretical and experimental results to generate the keys. The experimental result is located between the upper limit and lower limit.

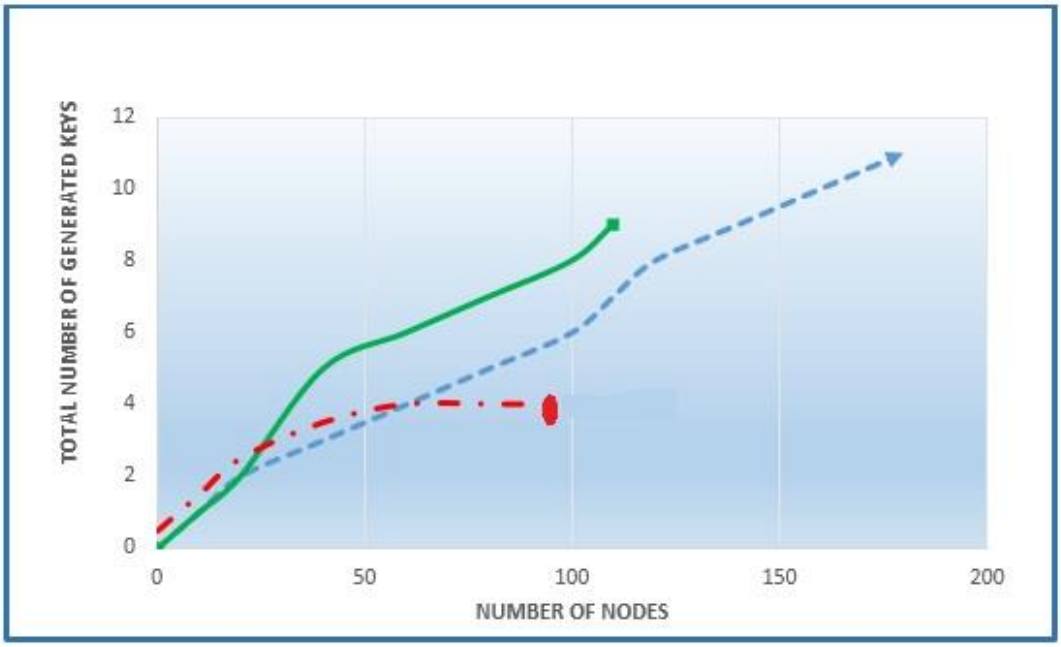


Figure (5.3) Generating keys.

The blue (dotted) line is the simulated results=176 keys , the green (solid) line is the theoretically calculated =110 keys upper limited values, and red (dashed) line is the theoretically calculated=70 lower limited values.

5.4 The Privacy of Experimental Results:

Assume RSB is compromised and Sybil attack gains the **coarse-grained hash** keys that is kept in RSB. In this case, the attacker knows only the **coarse-grained hash** values of all the keys. However, because it is shared among multiple nodes the knowledge of a node's **coarse-grained hash** value does not compromise its anonymity fully. Here, it is used the **k-anonymity** model in [54] for estimating the privacy. To avoid the unclear of ***k*** in the **k anonymity** with its keys, the name of the sample privacy it is **N anonymity**. To evaluate the privacy of nodes, it is produced keys for **256** nodes, and it is picked randomly the subset of nodes to check its anonymity. The results are appear in the figure (5.4). It appears the anonymity of the nodes which is closer to zero when the number of bits of **coarse-grained hash** values goes to 5. For more nodes, it expects a **coarse-grained hash** value that is necessary to reduce anonymity. For (2^24) nodes, it expects a 20-bit coarse-grained hash value that makes the anonymity = 0.(The expection for more nodes requires a longer coarse-grained hash to reduce the anonymity.)

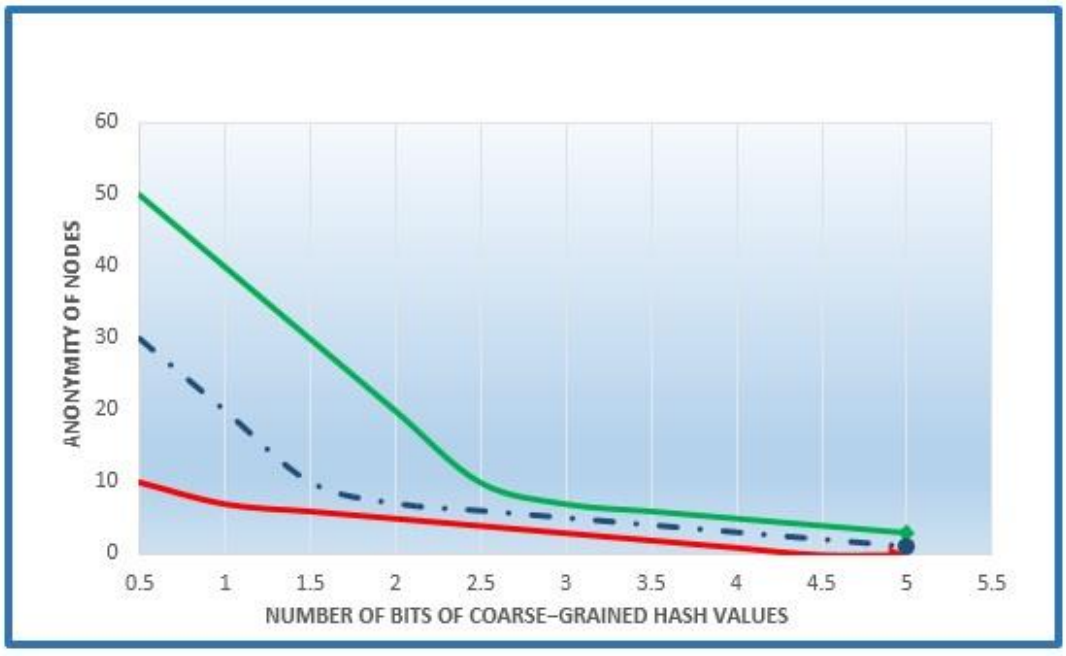
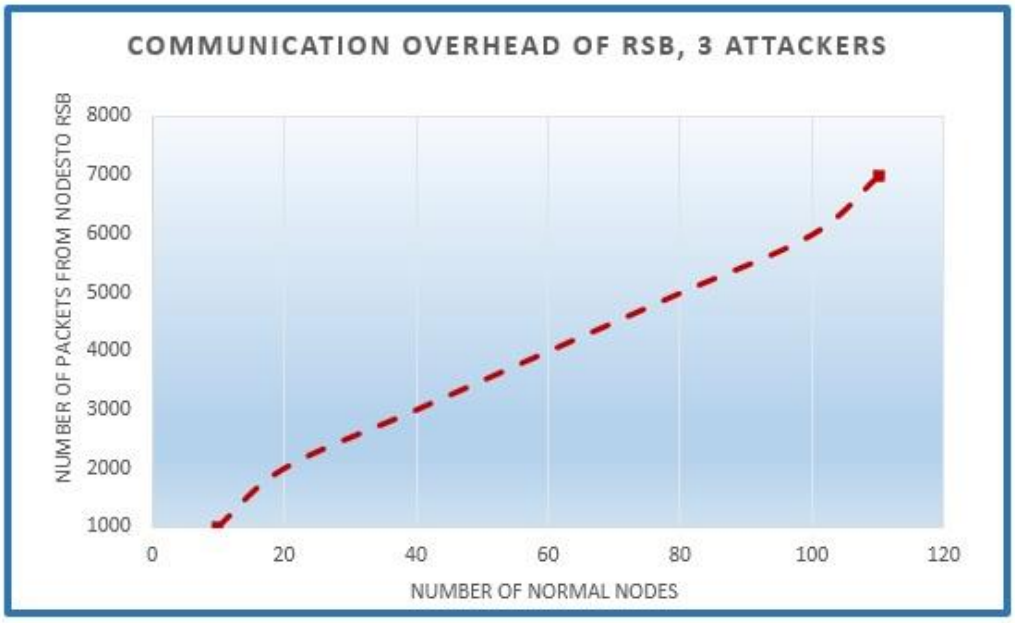


Figure (5.4) The anonymity of group of nodes

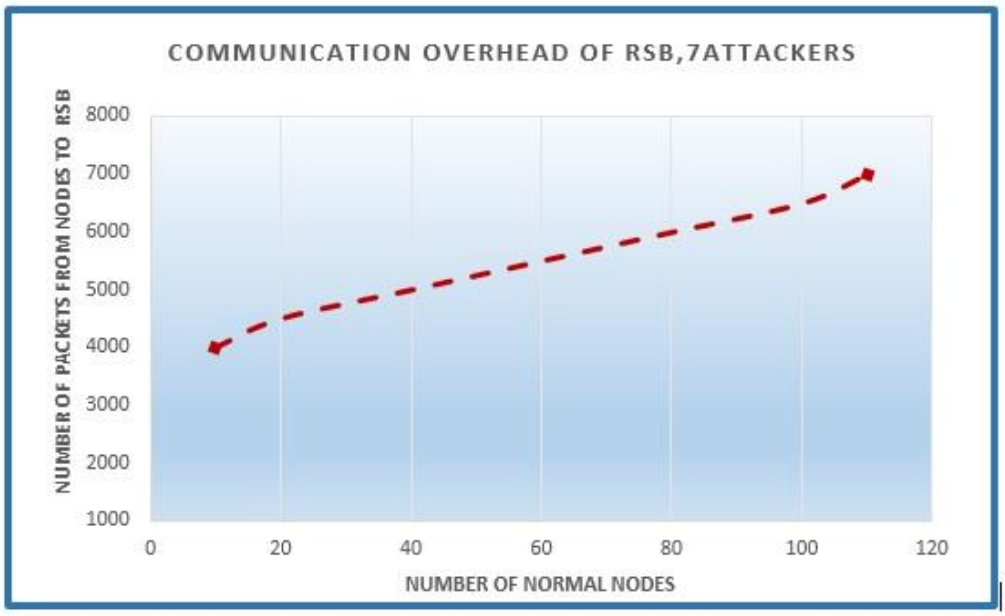
5.5 Communication Overhead in Experimental Results:

5.5.1 The Overhead on RSB:

In the figure (5.5) is explain the number of the packets that are treated by RSB. Through figure (5.5) the number of the packets that are received by RSB, it is increase with increase the sum of all attackers or sum of normal nodes.



(a)



(b)

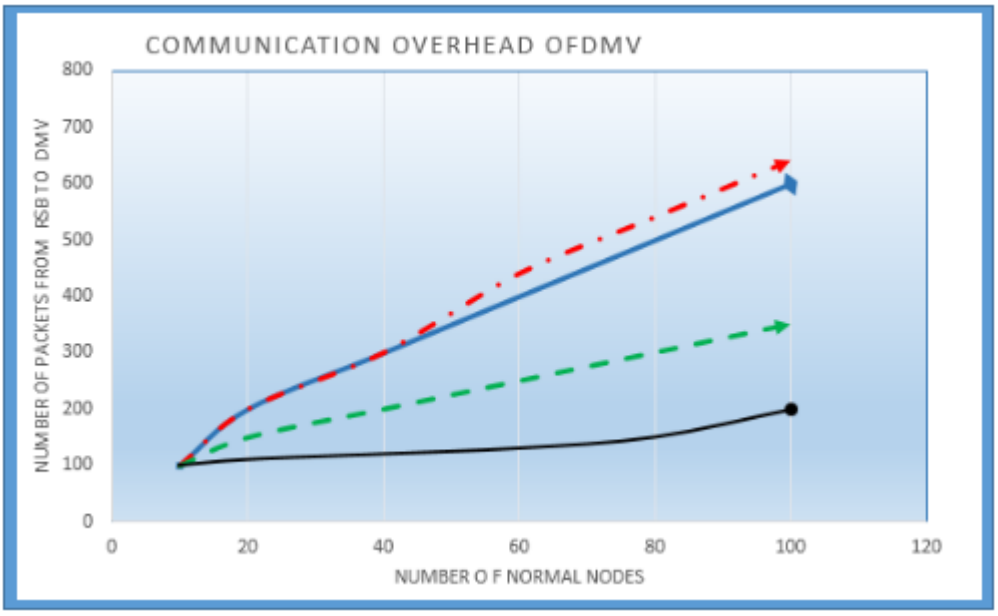
Figure (5.5) (a), (b) The number of packets from nodes to RSB

5.5.2 The Overhead on DMV:

The sum of packets that are sent to DMV it is exam, when RSB detects the malicious nodes it notifies DMV. The measurement is indicated of the transmission overhead over the wired network that connect RSB and DMV. The computation overhead of DMV is indicated by the number of the packets that are forwarded by RSB. Because DMV should process each packet for detecting Sybil attack. The results of packets that was sent from RSB to DMV appears in the figure (5.6). The conclusion of this figure, **if the number of coarse-grained hash values increases, the number of packets that transmitted increases.** In the figure (5.7), it is show the number of keys from RSB a little decrease when it increases the number of coarse-grained hash values. This result differs from the result that is appear in figure (5.6). There is concluded as the following:

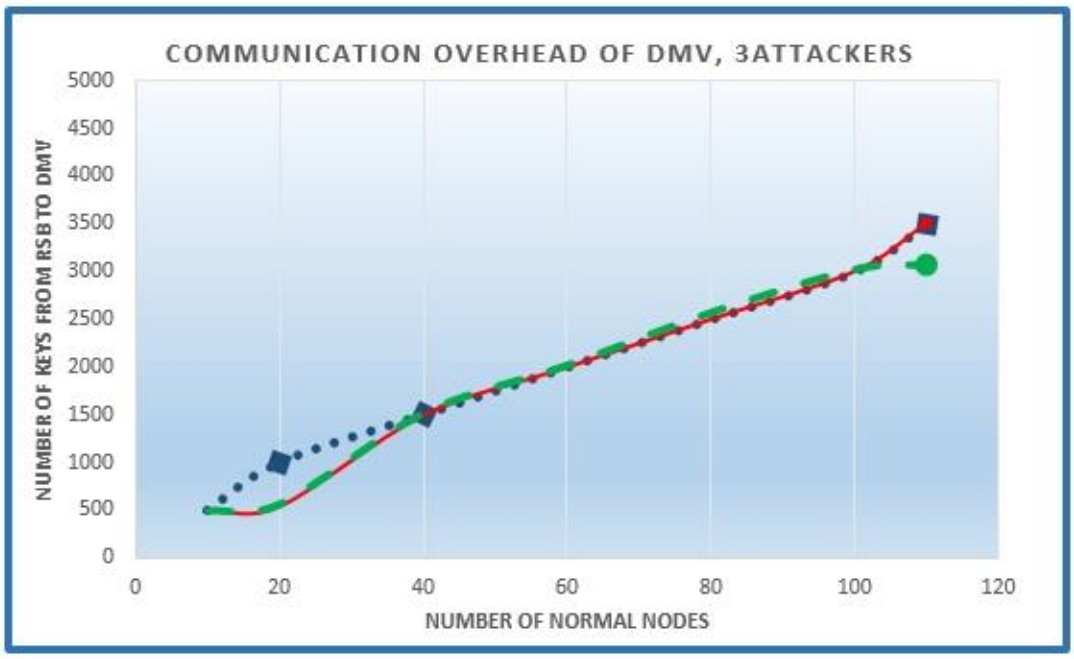
a) A large number of coarse-grained hash values, it is decrease of false alarms.

b) From figures (5.6), (5.7) the transmission overhead of DMV considers very big and causes complex computation overhead to DMV.



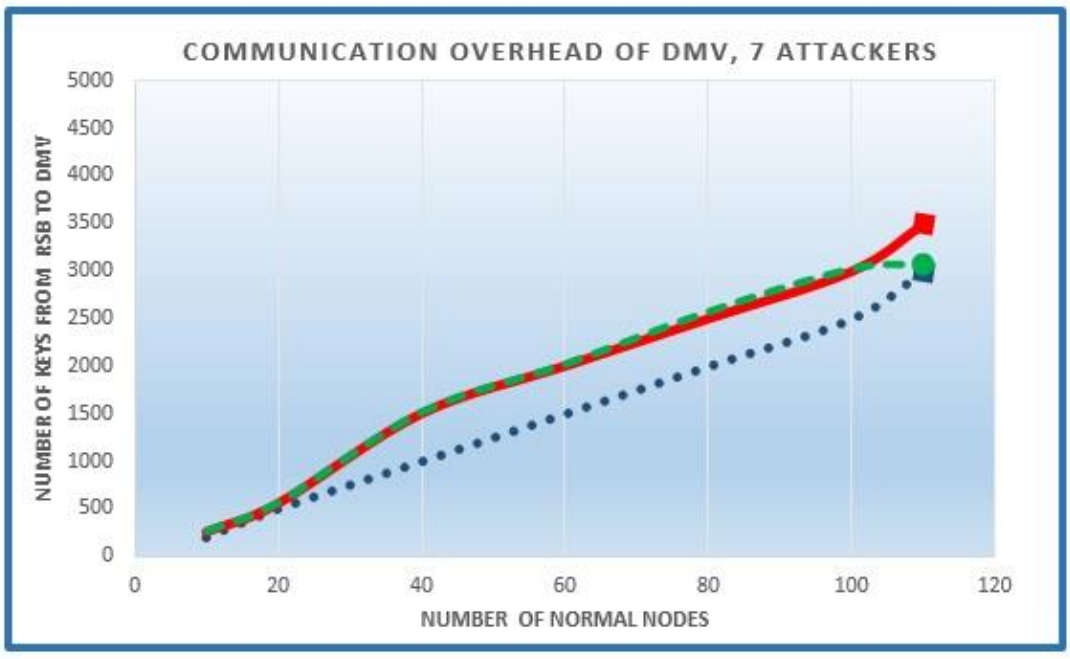
2 hash values=Black line(solid),4 hash values=Green line (dotted),8 hash values=Blue line (dashed),16 hash values=Red line (solid).

Figure (5.6) Number of packets sent from RSB to DMV



4 hash values=Green line (dashed), 8 hash values=Blue line (dotted), 16 hash values=Red line (solid).

(a)



4 hash values=Green line (dashed),8 hash values=Blue line (dotted),16 hash values=Red line (solid).

(b)

Figure (5.7) (a), (b) Number of keys between RSB and DMV

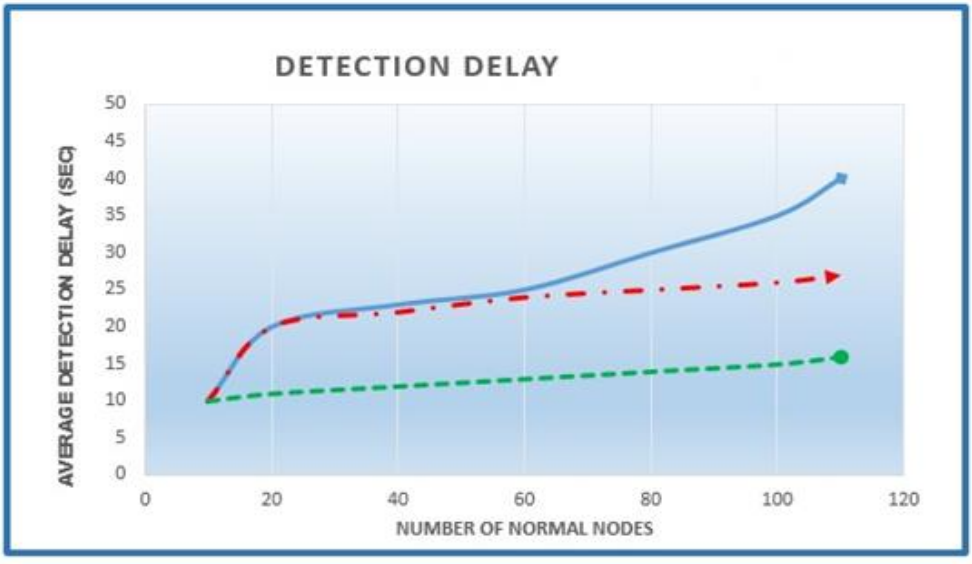
5.6 Latency for Detecting Sybil attack in Simulation:

In general ,the definition of latency is the delay from input into a system to required outcome.So, in the networks is a term of how much time it is take for a packet of data to obtain from one node to another. In this proposed method is assuming the latency Δt to detect Sybil attack is defined as T detect, T attack.

- **T detect**: considers the time which the attacker is detected by DMV.
- **T attack:** considers the time which the attacker first times attacks.

The proposed method is guarantee to detect Sybil attack when Δt is shortest. As is discussed before RSB can detect one malicious node in each period time. Thus, the initial time that an attack being hugged is in the next period time of that attack, and Δt is expected to be the length of the time interval. In Figure (5.8) it appears the result Δt for the propose method and it summarizes as following:

- The Δt increases when is increase the number of nodes. The Δt increases when increasing the number of Γ coarse-grained hash values.
- The Δt will be greater than length of the period of time when number of nodes is > 90.
- There are many differences because the large number of normal nodes that causes huge communication overhead on DMV.
- This overhead causes delay for RSB report because limited bandwidth between RSB and DMV.



2 hash values=Green line (dashed),8 hash values= Red line (dotted),16 hash values=Blue line (solid)

Figure (5.8) Detection latency

Chapter 6

Conclusions and Future Works

6.1 Conclusions:

This thesis focused on Sybil attack on wireless networks especially in (WSN and Ad hoc). This thesis addressed the advantage and disadvantage to the previous studies in wireless networks and depending on these studies to propose our method that is found in this thesis. The proposed method is to identify and avoiding Sybil attacks in VANET. The proposed method is based on cooperative between DMV and RSB to manage the network, and it release the little information based hash value. Also, DMV is responsible for all certificate authority (CA). Also is discoursed some developments on our scheme that is based on simulation results.

6.2 Future work:

There are many a good future works to develop the proposed method. Firstly, the prediction of the ratio and activities of Sybil attack. The estimation of the ratio of Sybil attack it makes the proposed method efficiently to detect the attack with low cost and delay. Secondly, DMV can be deployed to different areas which reduce the central management. Other future work creates more than RSB of the network.

REFERNCES

1. Akyildiz I, (2001) " Wireless sensor networks: a survey" Computer Networks 38 (2002) 393–422.
2. Olatunde A, et al, (2013) "Wireless Network Security: The Mobile Agent Approach" Int. J. Communications, Network and System Sciences, 2013, 6, 443-450.
3. Al-Sakib K, Hyung W, Choong S, (2011) "Security in Wireless Sensor Networks: Issues and Challenges" This work was supported by MIC and ITRC Project, ISBN 89-5519-129-4.
4. Naveed M, Islma M, (2015) "Detection of Sybil Attacks in Vehicular Ad Hoc Networks" Universal Journal of Communications and Network 3(1): 15-25, 2015, DOI: 10.13189/ujcn.2015.030103.
5. Tangpong A, (2010) "MANAGING SYBIL IDENTITIES IN DISTRIBUTED NETWORKS " Submitted in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy Doctor in Computer Science and Engineering.
6. M´onica D, (2006) " Thwarting The Sybil Attack in Wireless Ad Hoc Networks" This work was partially supported by FCT under grants PTDC/EIA/65588/2006 and PTDC/EIA/71752/2006.
7. Dhamodharan U, Vayanaperumal R, (2015)"Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method" Hindawi Publishing Corporation Scientific World JournalVolume 2015, Article ID 841267, 7 pages.
8. Piro C, Shields C, Levine B, (2015) "Detecting the Sybil Attack in Mobile Ad hoc Networks "This work was supported in part by NSF grants CNS-0133055, CNS -0534618, and CNS-0087639.
9. Yonglin R, (2012) "Towards Secure and Trustworthy Wireless Ad hoc Networks" Thesis submitted to the Faculty of graduate and Postdoctoral Studies In partial fulfillment of the requirements For the PhD degree in Computer Science .

10. Kumar U, Gambhi S, (2014) "A Literature Review of Security Threats to Wireless Networks " International Journal of Future Generation Communication and Networking Vol.7, No.4 (2014), pp.25-34

11. Anwar R, (2014)" Security Issues and Attacks in Wireless Sensor Network "world Applied Sciences Journal 30 (10): 1224-1227, 2014 ISSN 1818-4952© IDOSI Publications, 2014 .

12. Shukla J, Kumari B, (2013)"Security Threats and Defense Approaches in Wireless Sensor Networks: An Overview" International Journal of Application or Innovation in Engineering & Management (IJAIEM) ,ISSN 2319 – 4847

13. Alomari E, et al , (2012) " Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art" International Journal of Computer Applications (0975 – 8887) Volume 49– No.7, July 2012.

14. Pinkas B, Sander T, (2002) " Securing Passwords Against Dictionary Attacks " CCS'02, November 18–22, 2002, Washington, DC, USA.Copyright 2002 ACM 1-58113-612-9/02/0011.

15. Kaur J, Singh R, Kaur P, (2015) "Prevention of DDoS and Brute Force Attacks on Web Log Files using Combination of Genetic Algorithm and Feed forward Back Propagation Neural Network" International Journal of Computer Applications (0975 – 8887) Volume 120 – No.23, June 2015.

16. Abirami K, Santhi B, (2013)" Sybil attack in Wireless Sensor Network" International Journal of Engineering and Technology (IJET) ISSN : 0975-4024 Vol 5 No 2 Apr-May 2013 .

17. Newsome J,et al ,(2014) "The Sybil Attack in Sensor Networks: Analysis & Defenses" This research was supported in part by the Center for Computer and Communications Security at Carnegie Mellon under grant DAAD19-02-1-0389 from the Army Research Office IPSN'04, April 26–27, 2014, Berkeley, California, USA.Copyright 2014 ACM 1-58113-846-6/04/0004

18. Sharma K, Ghose M,(2010) "Wireless Sensor Networks: An overview on its Security Threats" IJCA Speci al Issue on "Mobile Ad-hoc Networks" MANETs, 2010 .

19. Chengwei H,(2016) " Research on Security Mechanisms for Wireless Sensor Network " International Journal of Future Generation Communication and Networking Vol. 9, No. 7 (2016), pp. 173-184 .

20. Arfat Y, Shaikh R,(2016)" A Survey on Secure Routing Protocols in Wireless Sensor Networks" I.J. Wireless and Microwave Technologies, 2016, 3, 9-19 Published Online May 2016 in MECS, DOI:10.5815/ijwmt.2016.03.02 .

21. Saxena S, Sejwar V, (2014)" Sybil Attack Detection and Analysis of Energy Consumption in Cluster Based Sensor Networks" International Journal of Grid Distribution Computing Vol.7, No.5 (2014), pp.15-30.

22. Niaz M, Saake G,(2015)" Merkle Hash Tree based Techniques for Data Integrity of Outsourced Data" 27th GI-Workshop on Foundations of Databases (Grundlagen von Datenbanken),26.05.2015 - 9.05.2015, Magdeburg, Germany.

23. Rathee P, Malhotra S,(2015) "Preventing Sybil Attack in Wireless Sensor Networks" IJIRST –International Journal for Innovative Research in Science & Technology| Volume 1 | Issue 12 | May 2015 ISSN (online): 2349-6010

24. Sharmila S, Umamaheswari G, (2012)" DETECTION OF SYBIL ATTACK IN MOBILE WIRELESS SENSOR NETWORKS" [IJESAT] INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY ISSN: 2250–3676 , Volume-2, Issue-2, 256 – 262.

25. Kumar M, Bhushan A, Kumar A, (2012) "A Study of wireless Ad-Hoc Network attack and Routing Protocol attack" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 4, April 2012 ISSN: 2277 128X .

26. AL-QAISI M,(2014) " Mobile Ad-hoc Networks for E-health Care Decision Support System "thesis submitted to the graduate school of natural and applied sciences of Cankaya university .

27. Karaoglu B,(2013) "Efficient Use of Resources in Mobile Ad Hoc Networks " Submitted in Partial Ful_llment of the Requirements for the Degree Doctor of Philosophy Department of Electrical and Computer Engineering Arts, Sciences and Engineering Edmund Hajim School of Engineering and Applied Sciences University of Rochester Rochester, New York 2013 .

28. Kaur S, Sharma C,(2013) " An Overview of Mobile Ad hoc Network: Application, Challenges and Comparison of Routing Protocols" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 5 (May. - Jun. 2013), PP 07-11.

29. Bhatti S, Sharma M,(2015) " A Review of Sybil Attack in Mobile Ad-hoc Network" International Journal of Advance Foundation And Research In Science & Engineering (IJAFRSE)Volume 1, Special Issue , ICCICT 2015. Impact Factor: 1.036, Science Central Value: 26.54

30. Sowmya P, Anitha V,(2014) " Defence Mechanism for SYBIL Attacks in MANETS using ABR Protocol" International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume-4 Number-2 Issue-15 June-2014 .

31. Vasudeva A, Sood M,(2012) " SYBIL ATTACK ON LOWEST ID CLUSTERING ALGORITHM IN THE MOBILE AD HOC NETWORK"

32. Pareek A, Sharma M,(2015)" Detection and Prevention of Sybil Attack in MANET using MAC Address" International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.5, September 2012.

33. Kamani J, Parikh D,(2015) " A Review on Sybil Attack Detection Techniques" Journal for Research| Volume 01| Issue 01 | March 2015 ISSN: 2395-7549.

34. Akshaya S, Thilagavathi D, (2015)" Survey on RSSI Based Sybil Defense" International Journal of Advanced Research in Computer and Communication Engineering ISSN (Online) 2278-1021,ISSN (Print) 2319-5940 ,Vol. 4, Issue 9, September 2015.

35. Rahbari M, Jamali M, (2011)" EFFICIENT DETECTION OF SYBIL ATTACK BASED ON CRYPTOGRAPHY IN VANET" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.

36. Zhou T, et al ,(2011)" P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 3, MARCH 2011.

37. Chang S,et al, (2011)" Footprint: Detecting Sybil Attacks in Urban Vehicular Networks" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, TPDS-2011-04-0199.R2 .

38. Lim k ,(2016) "Secure and Authenticated Message Dissemination in Vehicular ad hoc Networks and an Incentive-Based Architecture for Vehicular Cloud" Theses and Dissertations--Computer Science. Paper 48, University of Kentucky UKnowledge .

39. Sumathi M, Jothi S, (2015) "The Effectiveness of Route-Based Packet Filtering for Sybil Attack Prevention in Testbed Experiments", SSRG International Journal of Communication and Media Science (SSRG-IJCMS) – volume 2 Issue 1 January to February 2015.

40. Kumar S,et al ,(2010)" Routing Protocols in Wireless Sensor Networks A Survey", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010.

41. Akkaya K, Younis M,(2015) "A Survey on Routing Protocols for Wireless Sensor Networks" , International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2287-7970) Volume-4 Number-5 Issue-18 June-2015.

42. Krishna N, (2016) " Detection and Prevention of Sybil Attack in Networks" DOI 10.4010/2016.1013 ISSN 2321 3361 © 2016 IJESC

43. Al-Khafagey M,(2013) "Countermeasure to Black Hole attack in Mobile Ad hoc networks(MANET) " submitted to the council of the computer science in partial fulfillment of the requirement for the master degree.

44. Douceur R, (2002) "The Sybil Attack", IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems, pp. 251–260, Springer Verlag, London, UK.

45. Zhang Y, (2006) "Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006

46. Rida A, Young C, (2009) "Hop chains: Secure routing and the establishment of distinct identities", Theoretical Computer Science, 410 (6-7): 467-480.

47. Bhise A, Shailesh K,(2016)" Detection and Mitigation of Sybil Attack in Peer-to-peer Network ", I. J. Computer Network and Information Security, 2016, 9, 56-63 Published Online September 2016 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2016.09.08

48. Chris P, Shields C, Brian N,(2010) "Detecting the Sybil Attack in Mobile Ad hoc Networks", This work was supported in part by NSF grants CNS-0133055, CNS-0534618, and CNS-0087639.

49. Sukhpreet K , Chandan S,(2013)"An Overview of Mobile Ad hoc Network: Application, Challenges and Comparison of Routing Protocols" IOSR Journal of

Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 5 (May. - Jun. 2013), PP 07-11.

50. Saxena S, Sejwar V,(2014)"Sybil Attack Detection and Analysis of Energy Consumption in Cluster Based Sensor Networks", International Journal of Grid Distribution Computing Vol.7, No.5 (2014), pp.15-30 .

51. Bhatti S , Sharma M,(2015) "A Review of Sybil Attack in Mobile Ad-hoc Network"International Journal of Advance Foundation And Research In Science & Engineering (IJAFRSE)Volume 1, Special Issue, ICCICT 2015. Impact Factor: 1.036, Science Central Value: 26.54.

52. Jin H, Holz C,(2010) "Advances and Challenges in Ad-hoc Mobile Spatial Tracking for Seamless Interaction across Commodity Devices ", International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2287-7970) Volume-4 Number-5 Issue-18 June-2010.

53. Calandriello G,Papadimitratos P, Hubaux J, (2007)"Efficient and robust pseudonymous authentication in vanet," in ACM International Workshop on VehiculAr Inter-NETworking (VANET), 2007 .

54. Sweeney L,(2002) "k-anonymity: A model for protecting privacy," International Journal on Uncertainty, Fuzziness and Knowledge-based Systems,vol. 10, no. 5, pp. 557–570, 2002.

55. Manjunatha T, Sushma M, Shivakumar K, (2013) "Sybil Attack Detection Through On Demand Distance Vector Based Algorithm In Wireless Sensor Networks", Issue June 2013(JIARM).

56. Murat V, Youngwhan S,(2006) "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks" ,World of Wireless, Mobile and Multimedia Networks, WoWMoM 2006. International Symposium, 2006, pp.259-268

57. Zeng B, Chen B,(2010) SybilACO: Ant colony optimization in defending against Sybil attacks in the wireless Sensor Network, Issue 2010(IEEE).

58. Vamsi R , Kant K,(2016) "DETECTING SYBIL ATTACKS IN WIRELESS SENSOR NETWORKS USING SEQUENTIAL ANALYSIS , INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEMS VOL. 9, NO. 2, JUNE 2016

59. Lu R,(2012) "Security and Privacy Preservation in Vehicular Social Networks", Doctoral dissertation, University of Waterloo, 2012.

60. Chadha D,(2015)"Vehicular Ad Hoc Networks (VANET)", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 3, March 2015.

61. Kosch T,Strassberger M, (2004)" The role of new wireless technologies in automotive telematics and active safety" ,in 8th Symposium Mobile Communications in Transportation, 2004.

62. https://en.wikipedia.org/wiki/Wireless_sensor_network

63. https://en.wikipedia.org/wiki/SHA-1#SHA-0