Analysis of Black hole Attack in Ad hoc On-Demand Distance Vector (AODV) Routing Protocol:

Vehicular Ad-hoc Networks (VANET) Context

Master's Degree Program in Information Security and Cryptography

Networked Systems Security

Department of Future Technologies

Faculty of Science and Engineering

University of Turku

2019

Ranjam Alee

Supervisors:

Ethiopia Nigussie

Antti Hakala

UNIVERSITY OF TURKU
Network Systems Security / Faculty of Science and Engineering

ALEE RANJAM: Analysis of Black hole Attack in Ad hoc On-Demand Distance Vector (AODV) Routing Protocol: Vehicular Ad-hoc Networks (VANET) Context
Master's thesis, 68 p., 4 appendix pages
VANET System security
June 2019

In past years, popularity of Mobile Ad hoc Networks has led to the conception of Vehicular Ad hoc Networks. These networks must be highly secure before their implementation in real world. One of the vital aspects of these networks is routing protocol. Most of the protocols in VANET acknowledge all nodes in a network to be genuine by default. But there might be malicious nodes which can make the network vulnerable to various attacks. One such attacks is a black hole attack on AODV routing protocol. Because of its popularity, AODV and black hole attack are taken into consideration for this thesis.

The aim of the thesis is to analyze effects of black hole attack on AODV and understand security need of routing protocols in VANET. The experimentation for this thesis was performed with 40, 60 and 80 nodes in network simulator (NS). The performance metrics such as average throughput, end to end delay and packet delivery ratio of each assumed scenarios under blackhole attack and with prevention method are calculated. The obtained calculations are compared to analyze the network performance of AODV.

The results from the simulator demonstrate that overall network performance of AODV increased with black hole prevention algorithm in comparison to AODV under black hole attack only. Out of all the performance metrics that are used to analyze the network performance, the average throughput of AODV is significantly increased by 21 percent (approximately) when the mitigation algorithm is applied. The prevention approach used for the thesis can make AODV perform better against black hole attack. However, this approach is limited to a small to medium sized networks only.

Keywords: VANET, AODV, Black hole attack

Acronyms and abbreviations

ABID	Anomaly-Based Intrusion Detection
AODV	Ad-hoc On-demand Distance Vector
CAA	Colluding Adversary Attack
CCH	Control Channel
DDOS	Distributed Denial of Service
DOS	Denial of Services
DSRC	Dedicated Short Range Communication
DSSS	Direct Sequence Spread Spectrum
e2e	end-to-end
EDCA	Enhance Distributed Channel Access
ERDA	Enhance Route Discovery for AODV
ETSI	European Telecommunications Standard Institute
FCC	Federal Communication Commission
FHSS	Frequency Hopping Spread Spectrum
GPS	Global Positioning System
IDS	Intrusion Detection System
ISN	Initial Sequence Number
KBID	Knowledge-Based Intrusion Detection
LLC	Logical Link Control
MANET	Mobile Ad-hoc Network
NS	Network Simulator
OBU	On Board Units
OFDM	Orthogonal Frequency Division Multiplexing
PDR	Packet Delivery Ratio
RERR	Route Error
RREP	Route Reply
RREQ	Route Request
RSU	Road Side Units
SAA	Single Adversary Attack
SAODV	Secure AODV

SBID	Specification-Based Intrusion Detection
SCH	Service Channel
SSL	Secure Socket Layer
SUMO	Simulation of Urban Mobility
TCP	Transmission Control Protocol
TCP-F	Transmission Control Protocol Feedback
TIGER	Topologically Integrated Geographic Encoding and Referencing
TLS	Transport Layer Security
TraNS	Traffic and Network Simulation Environment
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VANET	Vehicular Ad-hoc Network
WAVE	Wireless Access in Vehicular Environment
WSA	WAVE Service Advertisement
WSMP	Wave Short Message Protocol

List of figures

List of tables

Table of contents

1. INTRODUCTION

The world of wireless system has been exponentially growing over the last decade. Wireless devices and wireless systems such as cell phones, PDAs, wireless computers, smartphones, etc. have been ubiquitous around our space in past years. Due to its convenient, portable and powerful nature, there is a rapid growth of such systems and hence ad-hoc networks are being more important in our lives. The definition of wireless ad-hoc network refers to the radio communication between various components of ad-hoc networks. These networks are infrastructure-less because of their mobile nature and therefore known as Mobile Ad-hoc Network (MANET). The popularity and convenient nature of MANET has inspired engineers and researchers to develop Vehicular Ad-hoc Networks (VANET) where vehicles will be able to communicate with each other autonomously. Although VANET has not been implemented in real world, there has been plenty of researches and experimentations going on to make it perform better and safer.

VANET, a subgroup of MANETs have similar features. The routing protocols used in MANETs such as AODV, DSR, ZRP and so on can also be used in VANET. Since most of these protocols were developed without regarding security, these protocols can be subject to various attacks and threats. An attack on the routing protocol can disrupt routing mechanism, eavesdropping of traffic data and even dismantle the whole network.

1.1 Motivation

People have always been commuting for work, study, shopping or for many different reasons. After the invention of cars, the mobility of humans has increased a lot. As a result, the traffic density has also increased. Such increase in traffic has certainly invited increase in number of road accidents and deaths. Because of such reasons, engineers are motivated to

develop an Intelligent Traffic System (ITS) which will reduce number of road fatalities, accidents and traffic jams. VANETs being a crucial part of ITS framework, it must be secure enough to fend off the possible threats and vulnerabilities.

Although all the layers of VANET's architecture must be robust and highly secure from attacks, the network layer is more prone to attacks and have higher degree of threats. Most of the routing protocols in MANETs have been used for over couple of decades, but their security is still under experimentation to make them more robust.

One of the most popularly used routing protocol in ad-hoc network is AODV. This protocol was designed without addressing security which is a vital aspect of any systems. AODV packets are not authenticated, encrypted or integrity checked at all. This opens up a numerous possibility of AODV message fabrication and interpolation using wide range of attacks such as DOS (Denial of Service) attack, wormhole attack, replay attack, grey hole attack, etc. One of the widely used attacks on reactive protocol like AODV is a black hole attack. Black hole attack is performed by abusing the route discovery mechanism in AODV. An attacker node misinforms other genuine nodes of having a best route to a destination and absorbs all the packets toward itself and dropping them eventually resulting in DOS attacks. Such nature of this attack awfully degrades the network performance by adversely affecting throughput, latency, bandwidth and other network metrics. In a VANET system where message dissemination must be fast, consistent and secure, a black hole attack on such system can disrupt the communication resulting in road injuries, major car accidents or even deaths. Therefore, highlighting and analyzing security issues of AODV in VANET system is one of the major motivations of this thesis.

1.2 Thesis Objectives

The main objectives of this thesis are to analyze the black hole attack against AODV routing protocol in VANET system and develop black hole attack mitigation technique. The thesis also explores the features of VANET system and various possible threats that can be launched on VANET. This thesis specifically deals with black hole attack and how AODV protocol can be secured from the attack on VANET. The proposed black hole attack

mitigation method is then implemented on AODV protocol and its performance is evaluated through simulation.

1.3 Thesis Structure

This thesis consists of many different chapters. The thesis structure is as follows:

Chapter 2. Literature review presents ad-hoc networks and their definition, security requirements and applications. Apart from these, it also introduces different communication types and standards for ad-hoc networks.

Chapter 3. Security problems in VANET explains possible threats and risks on different layers of VANET and the counter-measures to overcome those threats.

Chapter 4. Proposed black hole mitigating method discusses the black hole attack on VANET and proposes a simple method for preventing the attack.

Chapter 5. Implementation of AODV, black hole attack and proposed method describes various tools used, simulation environments and their setup. This chapter also illustrates parameters used for simulation and the performance metrics used for analyzing the simulation.

Chapter 6: Results and Discussion explains the results obtained from the simulation for various scenarios. It also presents result calculation and further discusses the performance of AODV under difference scenarios. Apart from this, this chapter also describes the limitations of the simulations.

Chapter 7. Conclusion summarizes the thesis work and highlights the importance of security of routing protocols for VANET system.

2. LITERATURE REVIEW

2.1 Ad-hoc networks: definition, features and applications

Mobile Ad-hoc Networks or MANETs have been a hot subject in a commercial research area. Previously used in military fields only, now gaining popularity in our daily lives. This network consists of many freely moving and independent nodes [1]. Every mobile node in this type of network acts as a router forwarding traffics to other targeted nodes [2]. A simple example of a MANET is shown in figure 2.1.

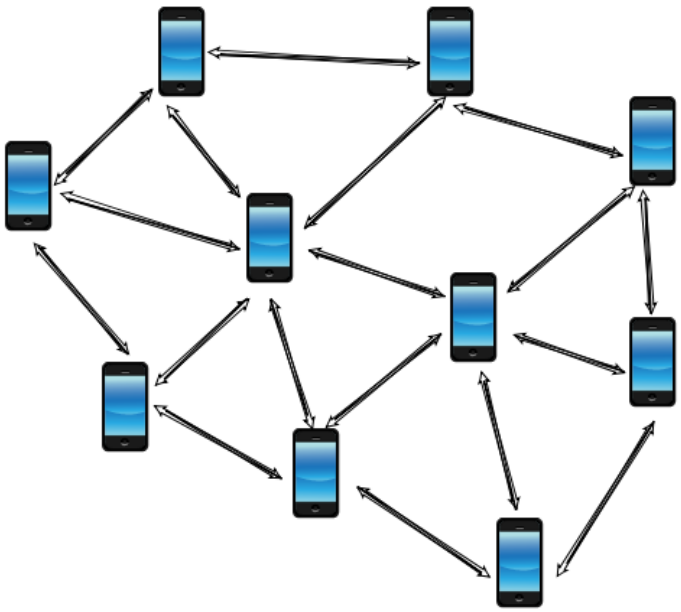

Fig 2.1: Mobile Ad hoc Network example

The evolution of MANET has led to the conception of VANET (Vehicular Ad-hoc Network). VANET is a network of autonomous vehicles and the roadside infrastructures constantly communicating with each other over a Dedicated Short-Range Communication

(DSRC) channel [3]. VANET is a type or subgroup of MANET with some distinct features. The distinctive features of VANETs are [2]:

- Highly Mobile: Compared to nodes in MANETs, VANET nodes are vehicles that move with high speed. This high mobility of VANET nodes causes many concerns.
- Highly dynamic network topology: Because of their high mobility, the network topologies in VANET frequently changes. This constant change in network topology made researchers and engineers to develop a special protocol that can perform well in highly dynamic and mobile network.
- Time critical: The exchange of information between the nodes must be quick. The time is critical in VANET as the messages must be transmitted fast and within the limit. A late arrival of warning messages can have a dangerous effect in the network.
- No power constraints: Unlike nodes in MANETs or other various networks, power is not a problem with nodes in VANETs. The nodes in VANETs are able to supply power to On Board Units (OBU) with the rechargeable battery present in a vehicle.
- Huge network size: The network size of the VANET will be huge. The network can scale from a highway to a city.
- Variable Network Density: VANET's network density changes with the density of traffics. The network density is less in countryside and high in traffic jam.

As mention earlier, a VANET system consists of vehicles and the road side units as shown in the figure below. The figure shows a continuous exchange of information between vehicles and towers (RSUs) [4].

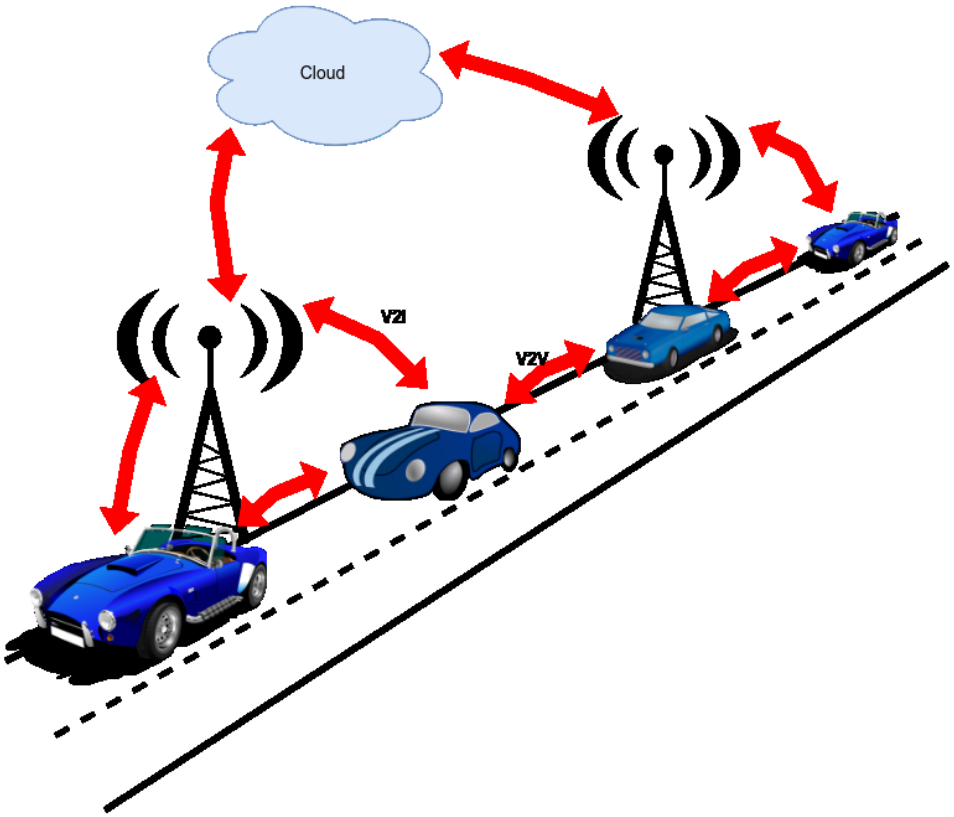

Fig. 2.2: Vehicular Ad hoc Network example

2.2 Communication types in VANET

VANET is a network of vehicles and infrastructure that are communicating with each other to provide safety on a road. VANET network consists of vehicles, which are mounted with on board units (OBU) and roadside units (RSU). These components are periodically sending and receiving messages with each other to form a safe, smooth and comfortable driving. VANET offers various application, which can be divided into safety application and non-safety application. Safety application includes emergency brake, light warnings, blind spot warning, etc. whereas non-safety application are related to infotainment for example weather forecast, internet access, etc. [5]

2. LITERATURE REVIEW

The communication types in VANET can be roughly differentiated into three types [6].

- Vehicle to Vehicle (V2V) communication: In this type of communication, vehicles like cars, trucks, vans, etc. embedded with on board unit exchange information with each other in an ad-hoc fashion. With the help of V2V communication, a vehicle can be able to identify the movement and the location of other vehicles within its range.

- Vehicle to Infrastructure (V2I) communication: In V2I communication vehicles can communicate with road side units (RSU) like a wireless LAN. In other words, in this type of communication architecture, vehicles can exchange data with road side infrastructure for instance traffic lights, towers, access points, etc.

- Hybrid Communication: Hybrid communication consists of both V2V and V2I communication. Vehicles are not only communicating with each other but also with RSUs in hybrid architecture. Figure 2.3 below depicts a communication flow between various components of a Wireless Access in Vehicular Environments (WAVE) system. WAVE is an architecture and standard developed for WAVE devices so that they can communicate in mobile environments.

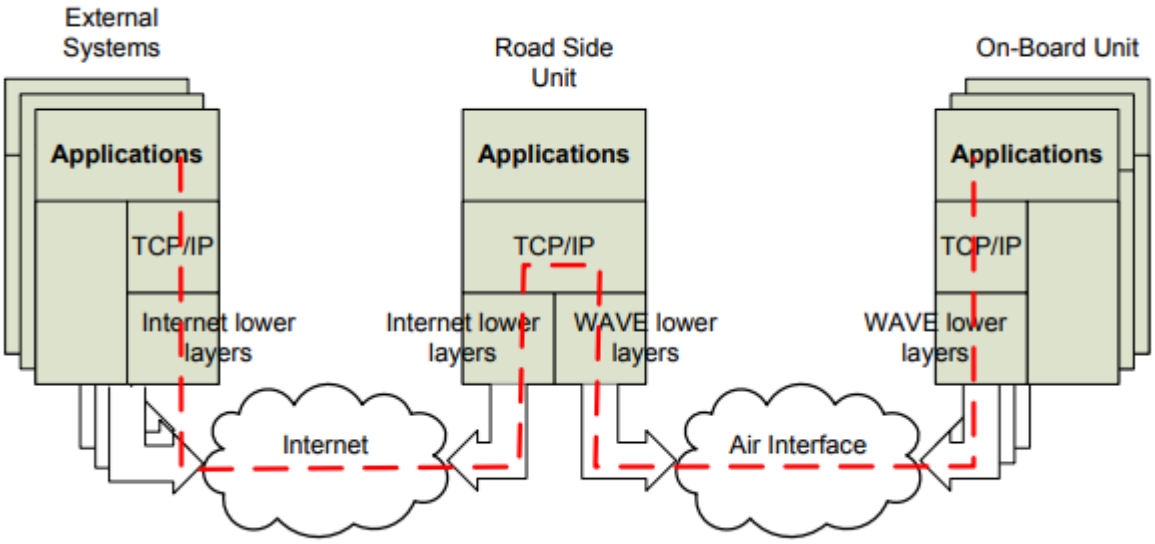

Fig. 2.3: WAVE system components [8]

2.3 Standards and Protocol for VANET

The distinct features of VANET demanded special standards which can perform well even in highly dynamic and highly mobile environment. This led to the development of WAVE (Wireless Access in Vehicular Environment) Standard. A WAVE standard is a radio communication standard, which was designed to provide interoperable and smooth services to VANET system. That means the wave devices can communicate with each other over a DSRC channel [8]. In US, Federal Communication Commission (FCC), has set aside a 75 MHz spectrum of 5.9 GHz frequency band for WAVE whereas the European Telecommunications Standard Institute (ETSI) in Europe has divided a 75 MHz frequency channel into seven channels, 10MHz each. Out of seven channels, one channel is used as control channel (CCH) and the rest six channels are configured as service channels (SCH). The CCH is used for carrying critical information while other non-critical or less priority information is sent over SCH. The current proposed DSRC/WAVE protocol stack consists of IEEE802.11p and IEEE1609 family which is the most mature standard for WAVE [5].

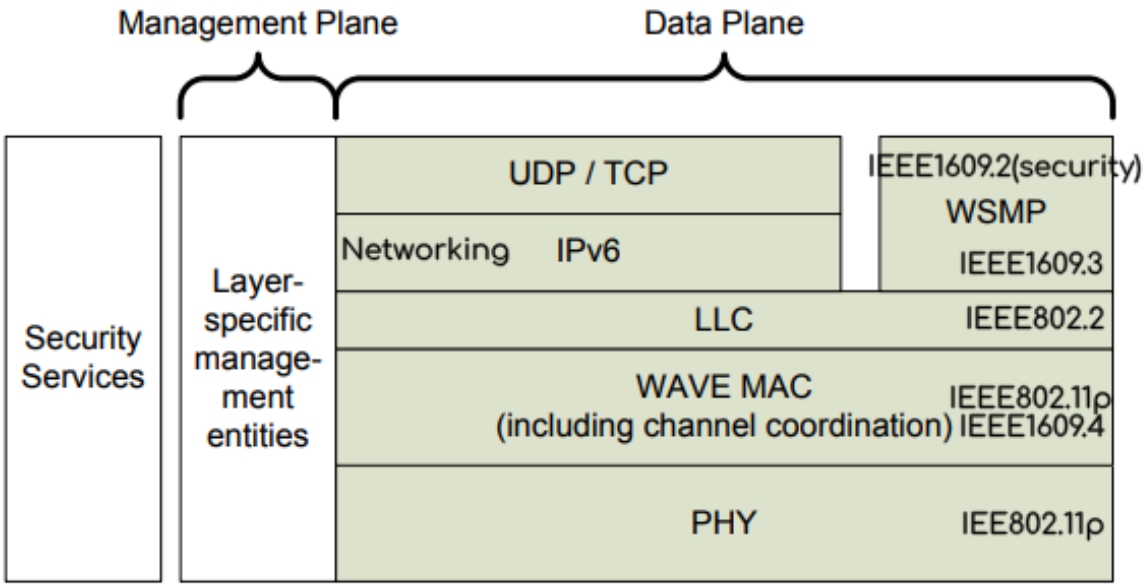

Fig. 2.4: protocols in WAVE stack [8]

2. LITERATURE REVIEW

WAVE PHY (IEEE 802.11p): IEEE 802.11p is an enhancement to IEEE802.11 standard. In contrast to IEEE802.11, only small changes are proposed in IEEE 802.11p. Some difference between these two standards are that the IEEE 802.11p uses OFDM (Orthogonal Frequency Division Multiplexing) mechanism over 10 MHz channels in 5.9 GHz band whereas, IEEE 802.11 or Wi-Fi uses OFDM PHY over a 20 MHz channels. The other difference is the carrier spacing in IEEE 802.11p is diminished to half than in IEEE 802.11 and the symbol length in 802.11 p is doubled to increase the signal strength from fading. IEEE 802.11p is implemented is PHY layer of WAVE architecture [8].

A distinct feature of this WAVE MAC is that it uses dynamic MAC addresses for OBUs. WAVE MAC (IEEE 802.11p/IEEE 1609.4): The MAC layer in WAVE should have the capability to handle the rapidly changing topologies induced by vehicles speed, huge density, and short connectivity and so on. Out of the many present radio standard, the simple yet popular and with high performance is IEEE 802.11 standard. In order to operate on multiple channels (SCHs and CCH), WAVE uses the concept of EDCA (Enhance Distributed Channel Access) technology. As shown in figure above, a WAVE reference model is composed of management plant and data plane. Data plane is responsible for providing data services while the management plane manages functions such as channel access, synchronization, etc. IEEE 1609.4 is used as an extension to IEEE 802.11p for channel management. Whenever LLC (logical link control) receives wave short message (WSM) or packets from higher layer, the LLC sublayer attaches an Ether Type value and forwards the data packet to the lower layers [11].

WAVE Network and Transport layer (IEEE Std. 1609.3): This Standard is used in DSRC/WAVE for Networking Services which illustrate WAVE network layer. There are two WAVE devices known as Provider device and User device. Provider device broadcasts WAVE Service Advertisement (WSA) on SCH to inform user devices of their service availability. The exchange of messages is performed using either of two protocol stacks; WSMP (Wave Short Message Protocol) or IPv6 protocol [11].

WSMP: Apart from IPv6 protocol operating on service channel, a WAVE network layer protocol that operate on both SCH as well as CCH. WSMP provides time critical and highly

important information. The primary objective for introduction of WSMP is to minimize overload. Broadcast Messages are traffic safety related messages and are broadcasted with the help of WSMs. These messages do not contain sensitive data and hence they are not encrypted but only signed by the sender's certificate [12].

WAVE Security services (IEEE Std. 1609.2): Safety is one of the critical aspects of a WAVE system. WAVE devices are prone to various vulnerabilities such as message spoofing, eavesdropping, message alteration and other various attacks. Such attack in one of the WAVE devices could cause a major accident. Hence, this Standard explains the various security measures implemented to secure the message exchange between WAVE devices.
Apart from the above-mentioned standard, there are many other standard of 1609 family which are under research and experimentation for various purposes. For instance, IEEE1609.11 is the standard for electronic payment system, IEEE1609.12 will be used for Identifier Allocation [12]

2.4 Security Requirements of VANET

A system can be vulnerable to various system weaknesses which can be exploited by malicious element for various reasons. To make a system secure, security requirements of a system must be addressed. There are some security requirements of VANET system which are briefly described below. Also, the figure 2.5 shows the kinds of possible attacks that can compromise security requirements in VANET [13].

Authentication: one of the major and indisputable requirements of any system. A system must know the authenticity of all the participants of the system. Especially, in VANET which is vulnerable to various exploits, the authentication and identification becomes very important and necessary. In case of some attacks in VANET, powerful authentication approach can provide a strong legal proof against the intruder. Hence, to protect VANET system from attacks such as Sybil attack, position attack, tunneling, replay attack, message alteration and so on, Authentication process is an obvious requirement.

Availability: a system or a component in a system might face failure or some attacks. Such malicious condition of a component or a system should not affect other users or element of the system. In VANETs, all the applications and network should be available and function even when a n element of VANET is under attack. Some VANET nodes or infrastructure might face some attacks or issues which should not affect other nodes. In other words, the resources of VANET must be always available. To achieve the availability requirement in VANET, a robust, secure and tamper tolerant system design must be achieved. There are various attacks like Denial of Services (DOS) attack, Black hole attack, spamming attack, Distributed Denial of Service (DDOS) attacks, etc. that can have a serious impact on the availability requirement of VANET.

Confidentiality: refers to the privacy of confidential information of a node or an infrastructure. The messages exchange between two components in VANET should not be exposed to third entity. Confidentiality can be achieved by using various encryption algorithms. In VANET, the safety messages do not possess sensitive data hence they are not encrypted. However, the user related information such as electronic payment, user's identity and other personal information are kept confidential with the help of various cryptographic algorithms. Traffic analysis, Data spoofing and eavesdropping are some of the potential attacks on confidentiality in VANET.

Integrity: protects messages from fabrication or interpolation. The messages sent and received by various entities of VANET should be kept intact. Which means the integrity of messages must be protected from being tampered by attackers. Integrity of messages can be affected by attacks such as Masquerade attack, Replay attack, Data alteration attacks, etc. To safeguard messages during transmission and reception, a secure protocol must be implemented. In VANET, IEEE1609.2 standard is used for security services.

Non-Repudiation: one of the important security requirements of VANET. Non-Repudiation ensures a sender or a receiver from denial of the transmitted data from

them [16]. VANET security requirements and the possible threats to those requirements is outlined in figure 2.5 below.

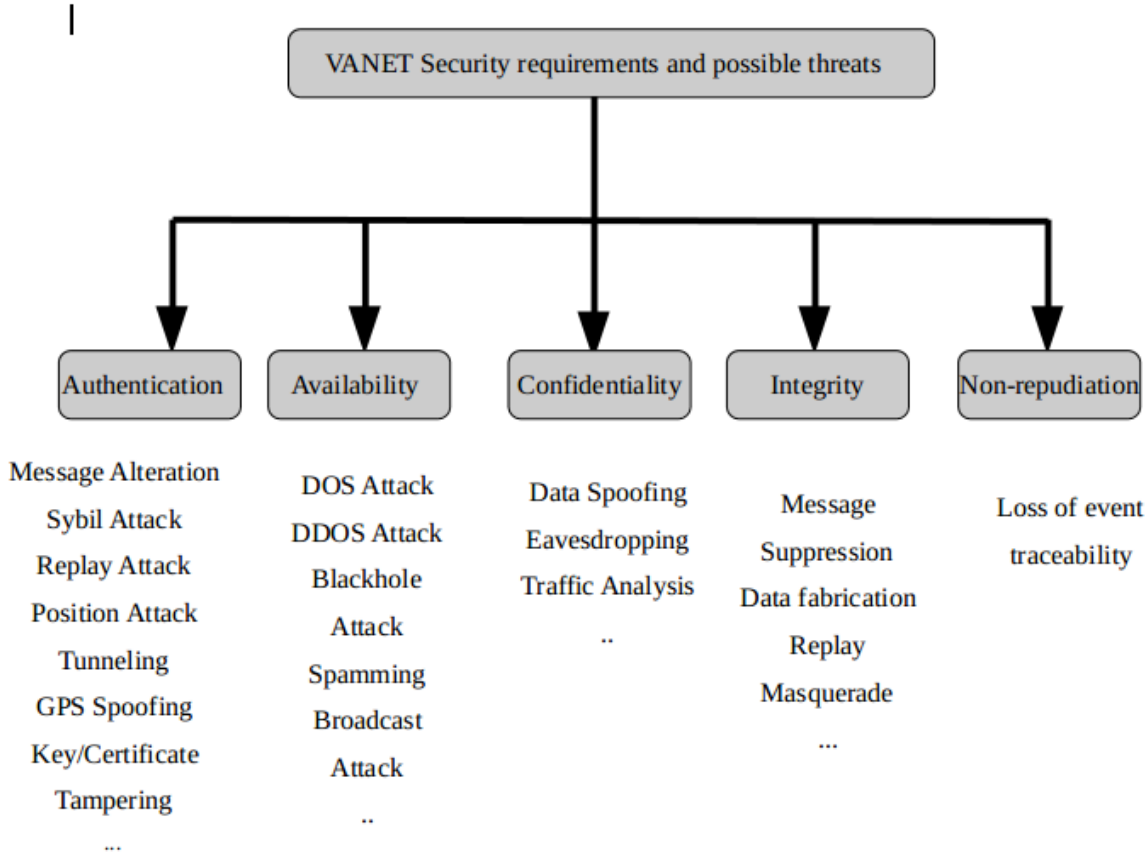

Fig. 2.5: VANET security requirements and possible threats [5]

2.5 Routing Protocols

Routing protocol for ad-hoc networks has been studied extensively in the last decades. Many ad-hoc routing protocols have been designed, developed and experimented with MANETs for different scenarios. Since VANET is a type of MANET, the routing protocols used in MANETs are assessed and evaluated to be implemented for VANETs too. Based on these routing protocol's route updating method and position accusation, the routing protocols have been divided into five different categories [17]. They are as follows:

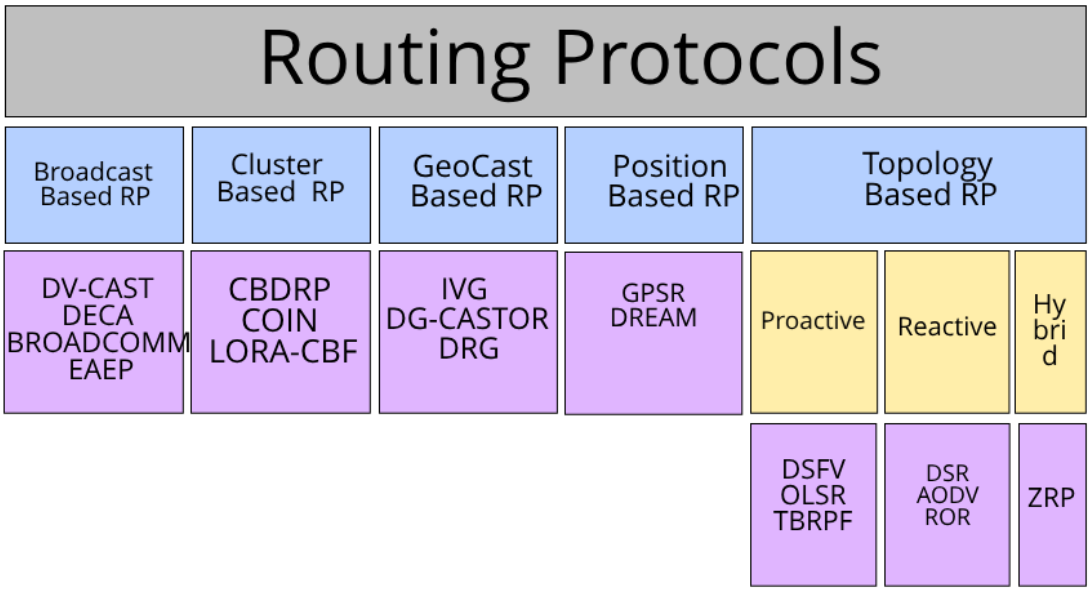

Fig. 2.6: Routing protocols hierarchy [17]

2.5.1 Broadcast Based Routing Protocols

Broadcast based routing protocols broadcast the packet to all the nodes within its vicinity. If a node wants to send data to a destination node outside of its transmission range, then this method of broadcasting becomes handy. In VANET, mostly safety related data such as traffic condition, weather forecast, road traffic warning, etc. are broadcasted using broadcast-based routing protocols [17].

2.5.2 Cluster Based Routing Protocols

Clustering is a method of grouping nodes with similar properties such as direction, speed, etc. into groups or cluster. Every cluster contains a cluster-head whose main function is to

transmit data between nodes using gateway nodes. Although network overhead grows with the use of Cluster based routing protocol, but it is highly scalable when it comes to huge networks.

2.5.3 GeoCast Based Routing Protocols

GeoCast Based Routing Protocol transfers data to a collection of nodes located in a certain geographic location. Even in rapidly changing network topology, these routing protocols deliver packets reliably. Some examples of these type protocols are DG-CASTOR, IVG, etc.

2.5.4 Position Based Routing Protocols

These protocols use location-based services like GPS (Global Positioning System) to transmit data from source to destination. Like other protocols, position-based routing protocols does not require route creation and therefore does not need route maintenance. The performance of such protocols is high in highways where the vehicles are travelling with huge speed.

2.5.5 Topology Based Routing Protocols

In these type of routing protocols, packet forwarding from source to destination is performed by utilizing the accessible information of links that inhabit within the network. These routing protocols have a capability of sending unicast, multicast and broadcast messages to other nodes. Apart from this, they consume less resources and low bandwidth. They are further sub grouped into three categories:

- Proactive Routing
- Reactive routing
- Hybrid routing

The scope of this thesis is to study one of the popular reactive routing protocols, Ad hoc On-demand Distance Vector (AODV) routing protocol. Therefore, it only explains AODV routing protocol in details. The next topic discusses AODV and how it functions.

2.6 AODV routing protocol

AODV is an improvement of DSDV routing protocol and one of the most popular routing protocols in ad-hoc networks. AODV protocol utilizes the DSDV's algorithm by reducing the broadcasts and establishing routes only when demanded or needed. Because of such characteristics of AODV, superfluous memory and route redundancy are curtailed and hence it is suitable for VANETs also.

As in most of the reactive protocols, the data transmission occurs in AODV only in an on-demand state. AODV performs unicast as well as multicast operations [11]. In General, AODV takes two steps for operation which are as follows:

2.6.1 Route Discovery Process

When a source node needs to establish a path to a destination node, the sending node floods the neighboring nodes with a Route Request (RREQ) message. This RREQ messages are broadcasted further by the neighboring nodes until the destination node is found or an intermediate node with a path to destination is found. To prevent loop, every node manages broadcastID and SequenceNumber. The broadcastID and sourceID identifies a RREQ packet uniquely. Therefore, every time a RREQ message is received by a node, the broadcastID is incremented. Multiple copies of RREQ message with same source IP address and broadcastID (RREQ ID) are received by the intermediate nodes, these RREQ packets are discarded without forwarding. Table 2.1 illustrates an AODV RREQ packet format [11].

Table 2.1: AODV RREQ packet format [11]

Type	Reserved	Hop Count
RREQ ID		
Destination IP address		
Destination Sequence Number		
Source IP address		
Source Sequence Number		

Once the destination node or an intermediate node with the route to destination is found, the node then creates a RREP (Route Reply) message and sends to the path back to the source node. The intermediate node receiving RREP message update their routing tables for the future use. The multiple duplicate copies of RREP message are discarded by comparing the broadcastID and source IP address. There is a possibility of receiving RREP message by source from multiple nodes. The source node updates its routing table with the new recent route by using the highest destination sequence number. The table below depicts an RREP packet format of AODV routing protocol [11].

Table 2.2: AODV RREP packet format [11]

Type	Reserved	Prefix size	Hop Count
Destination IP address			
Destination Sequence Number			
Source IP address			
Lifetime			

2.6.2 Route maintaining process (Link failure)

Every neighboring node in the network periodically exchange HELLO messages with each other. A sign of link failure can be absence of HELLO messages. If a node has not received HELLO messages until a designated time, then the node is marked as unreachable resulting in link failure. Once link failure occurs, every active neighbor is notified by sending Route Error (RERR) message. Router error message is initiated by the node closer to the Source node of the linked failure [11]. A simple example of AODV operations can be seen in the figure below.

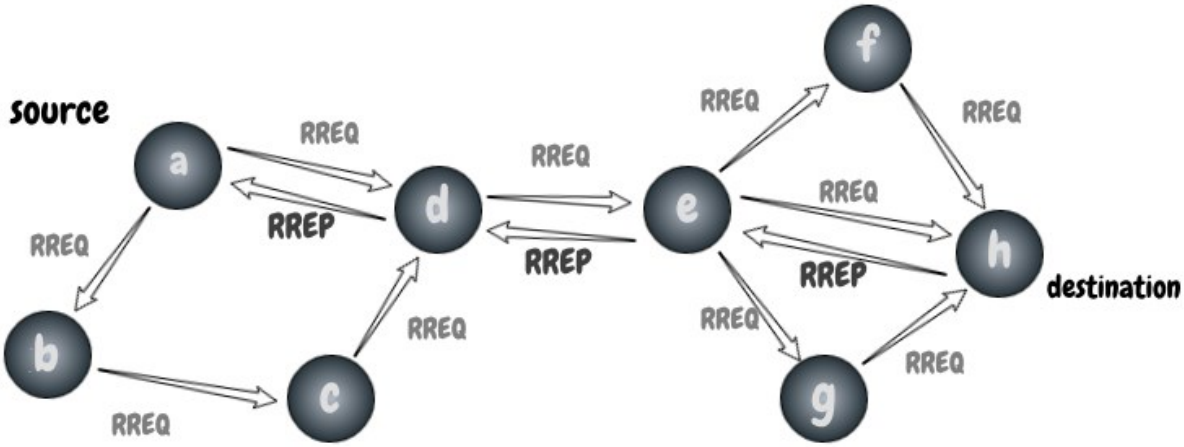

Fig. 2.7: AODV Routing Protocol

3. SECURITY ISSUES IN VANET

Although VANET technology has improved and developed in recent times, there are still many security issues that exists in the system. Small error in a software application can cause serious consequences in the VANET system. The security aspect of VANET is a huge challenge to secure VANET from various attacks, privacy issues and information leakage.

VANET still has many vulnerabilities which can be exploited by the attackers. Before adoption of VANET in real world, the different layers of VANET must be made secure. There are various threats and attacks that are present in different layers of VANET system. The topic below addresses some of the possible attacks on the WAVE layers in VANET and provides countermeasures briefly that can be applied to mitigate those security issues [21].

3.1 Application layer (attacks and countermeasures)

In VANET, an application Layer is responsible for the users' information that are related to applications such as Email, Web, etc. The Applications on this layer use various application level protocols like HTTP, FTP, SMTP, etc. which can be exploited by the attacker for various reasons. Some of the main attacks on this layer in VANET are:

Malicious Code: an attacker can circulate malicious code to other vehicles or to RSU to disrupt or impair an application in a VANET. Malicious code can include viruses, malware, spyware, Trojan horses, etc. which can have an adverse effect in the application layer. Using such codes, attacker can dismantle the system or gain user related information from an infected vehicle.

Repudiation or message falsification attacks: in this type attack, an attacker captures the message via the wireless medium and manipulates the message and rebroadcast them. Altering content of messages can have an adverse effect on the system. Hence, such attack can cause misleading or invalidation of data in VANET.

Countermeasures

Various anti-virus and anti-spyware software can be installed for VANET application which can protect against viruses and spywares. Programs like Firewall which monitors inbound and outbound traffics can be effective as a major countermeasure against application layer attacks. Apart from this, IDS (Intrusion Detection System) can be implemented to fight against spoofing and abnormal activity.

3.2 Transport Layer (attacks and countermeasures)

Transport layer in VANET deals with the end-to-end communication in a network. This layer facilitates with logical communication between application layer and network layer. There exist security concerns such as secure end-to-end communication, authentication etc. in transport layer for VANET. Some of the possible attacks that VANET confront on this layer are:

Session Hijacking: an attacker gains control over the session between two entities. Since Authentication process is performed only at the beginning of a session. Once authenticated, the attacker masquerade as one of the authenticated members of the VANET network and seize control over the session.

SYN flooding: TCP protocol uses three-way handshake to establish a connection between nodes. To establish a connection, a sender node sends SYN packet to the receiver along with Initial Sequence Number (ISN). Upon reception of SYN packet, the receiver node acknowledges by replying with ACK and SYN packet. Finally, the sender node sends an ACK packet and the connection is established. An attacker can generate numerous half-opened connections between two nodes known as SYN flooding. It is a type of DOS attack.

Countermeasures

TCP is not appropriate for MANET. And hence not suitable for VANET too. Although TCP-F (TCP feedback), ATP (Ad-hoc Transport Protocol), etc. are implemented in MANET, these protocols do not reduce the transport layer issues in MANET. Those protocols will also not be appropriate for VANET. However, some protocols such as TLS/SSL (Transport Layer Security/ Secure Socket Layer) helps prevent attacks like replay attack, masquerade attack and man-in-middle attack.

3.3 Network Layer (attacks and countermeasures)

Compared to Application layer attack in VANET, network layer attack can affect more nodes or even the whole network system. Especially in VANET, due to its dynamic topology, it is difficult to maintain routes. The components of VANET acts like a router and an attack on any of its component can dismantle the whole network. There are many routing protocols developed but each protocol has its own security issues. Basically, the attacks on routing protocol are divided into active attack and passive attack.

Active attacks are those type of attacks, which halts the functioning of a routing protocols. Whereas passive attacks do not halt the operation of protocol but are launched to steal routing information or traffics. Some of the attacks on network layers are:

Routing table overflow: this type of attack causes the overflow of routing table in VANET. In other words, an attacker advertises routes to nonexistent nodes to legitimate nodes. Because of this, routing protocol are not able to register new legitimate routes in their routing table. Proactive routing protocols such as DSFV, OLSR are affected by such attack as they update their routing information regularly.

Route cache poisoning: on-demand routing protocol such as DSR, AODV stores information about recent routes in their route cache. The information can be removed, changed or altered with incorrect information.

Byzantine attacks: this type of attack occurs where an attacker gains complete control over most of the legitimate nodes of a VANET system. A victim node then performs many malicious activities like dropping packets, generating routing loops and so on which degenerates the routing function. Byzantine attacks are carried out by a single malicious attacker or a by a group of organized malicious nodes.

Rushing attacks: has capability to pass forth route reply (RREP) packets faster than the authenticated nodes in a VANET. This creates an opportunity for the adversary to establish a path through it rather than the authenticated nodes. Mostly reactive protocols like AODV, DSR are the victim of such attack. This attack can result in the DOS attack and can dismantle a VANET network.

Sybil attacks: In a VANET system, every node is authenticated and identified uniquely. A malicious node can create multiple virtual identities which is called Sybil attack. This attack creates an illusion among the legitimate nodes that those virtually created nodes exists physically. It is one of the attacks which cannot be detected easily.

Sinkhole attacks: In a VANET, an attacker advertises to other nodes of having a better and legitimate route to the destination node. Once the source starts sending data via the route advertised by the attacker, forwarding of the data never occurs. Hence known as sinkhole attack.

Wormhole attacks: It is one of the dangerous attacks that is very difficult to prevent. Wormhole can be very devastating even when the security scheme like authentication and encryption are implemented. Although this type of attack can be performed by a single node but usually, they are carried out by two or more malicious nodes.

Attackers create a tunnel known as wormhole link which captures traffics from one end and send them to another end.

Black hole attacks: A black hole attack is an attack against integrity of network in VANET. This type of attack is launched in two steps. First, an attacker node misuse protocols like AODV by advertising itself of having a better route to destination node. The node captures packets and drops them in second steps. As black hole attack is the focus of the thesis, it is explained in detail in later chapter.

Countermeasures

The countermeasures of network layer attacks mostly depend on the type of routing protocol used in VANET. In general, various security mechanism such as cryptography-based algorithm, trust-based approach can be implemented to defend against attacks on network layer. Since this thesis deals with the black hole attack on AODV routing protocol, a sequence based approach is adopted and it is explored in details in chapter 4.

3.4 MAC layer (attack and countermeasures)

The MAC layer (also physical layer) in WAVE uses IEEE 802.11p standard. This standard makes use of CSMA/CA to supply channel access and curtail collisions. An Attack on MAC layer can result in the disruption of the channel access mechanism. It can cause exhaustion of bandwidth and even power which in turn produce low throughput in network. Some of the major attacks on MAC protocols such as IEEE 802.11a and IEEE 802.11p are DOS and DDOS attack. According to Zhou, Wu and Nettles [1] two MAC layer DOS attacks can be carried out namely single adversary attack (SAA) and colluding adversary attack (CAA).

Countermeasures

SAA attack on MAC can be defended using the proposed packet-by-packet authentication scheme in [1].

CAA attack can be prevented using the approaches like distance adjustment, protecting flow of traffic, etc.

3.5 Physical layer (attacks and countermeasures)

There are various attacks that can be launched on physical layers. For instance, jamming, eavesdropping, interference, etc. A malicious node can perform eavesdropping by intercepting the messages over the air using special receivers. The radio waves transmitted by nodes antenna can be jammed and interfered by strong signals generated from transmitter. This can cause the messages to be discarded or corrupt.

Countermeasures

Spread spectrum technique adjusts radio frequency in a random fashion which creates difficulty to jam radio signals. Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) technique can be implemented to mitigate physical layer attack.

4. PROPOSED METHOD TO MITIGATE BLACK HOLE

As mentioned before, most of the routing protocols for Ad-hoc networks were developed long time ago without considering their security mechanism. Hence, those routing protocols are prone to various attacks. As black hole attack mitigation in AODV routing protocol is one of the objectives of the thesis, a sequence number based black hole mitigation method is developed and presented in this chapter. Existing approaches on black hole prevention on AODV are also studied in this chapter.

4.1 Black hole attack (on AODV)

Black hole attack is a kind of attack where a malicious node attempts to capture all or most of the traffics toward itself by broadcasting bogus routing information to its neighboring nodes. In AODV routing protocol, when a node wants to send data to a destination node, it initiates a route discovery process by sending RREQ packets to its neighboring nodes. When a node with malicious intent receives the route request (RREQ) packet, it then replies with a highest sequence number claiming that it possesses a best route to destination. After the source node has received RREP from the attacker node, it starts sending data to the attacker node. Once the attacker node starts receiving data, it can perform selective forwarding or just dropping all the data.

As it can be seen in the figure below, node A(source) wants to send data to node H(destination), it sends RREQ packets to its neighboring nodes B, C and D. Node B, being an attacker node sends route reply packet (RREP) with highest sequence number. Source node A also receives RREP via H-F-D-A and H-E-C-A. But source node A finds route via B to have better metric than other routes and hence forwards all the data via node B. Node B drops all the data it has received without forwarding the data to its neighboring nodes.

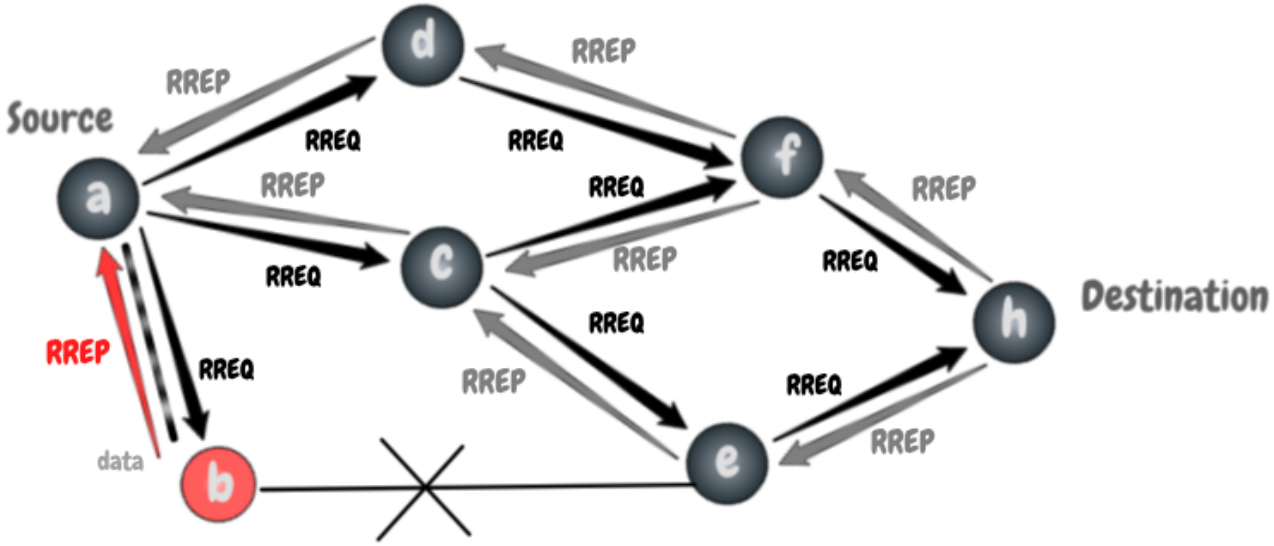

Fig. 4.1: Black hole attack

4.2 Existing black hole attack mitigation schemes

Trust based Routing

Fidel Thachil and K.C. Shet et al. [29] proposes a trust based approach for AODV protocol to mitigate black hole attack. In this approach, all nodes maintain a trust value of their neighboring nodes by listening to their neighbors promiscuously. The trust value is calculated dynamically. Whenever the trust value of any node drops below a predefined threshold trust, the node is supposed to be a malicious one and thus it is averted from route.

IDS (Intrusion Detection System)

Adnan Nadeem and Michael P. Howarth et al. [28] explains in their survey various intrusion and detection approaches than can be implemented in MANETs. Based on the detection method application, the survey categories the intrusion detection techniques into three main classes. They are Anomaly-Based Intrusion Detection (ABID), Knowledge-Based Intrusion Detection (KBID) and Specification-Based Intrusion Detection (SBID).

Watch Dog Mechanism

This mechanism helps to identify any misbehaving nodes in a network [27]. The basic working principal of watchdog mechanism is by watching the neighboring node with the help of previously sent messages in the buffer. Whenever a node forwards a message, the watchdog makes sure that the next node in the network way also forwards the message. The watchdog achieves this process by promiscuously listening to the nodes within its range. Whenever a watchdog finds a message not being forwarded by any of its neighboring node or forwarded by modification, it is believed to be misbehaving. And if a node only receives packets but doesn't forward the packets or message, then the node is marked as a malicious node.

ERDA (Enhance Route Discovery for AODV)

Kamarularifin A.J, Zaid A. and Jamalul-Lail A M. et al. [34] proposes an enhanced method of route discovery in AODV protocol by addressing low overheads. This method consists of two-part process. In first part, a new parameter is added in order to secure routing table update. In second part, Receive Reply packets stored in a table is inspected to remove any malicious nodes. ERDA is secure and has low latency compared to other methods.

Secure AODV (SAODV)

A Secure AODV or SAODV is another approach to make AODV routing protocol more secure. It is an enhancement of AODV protocol. The probability of attack in SAODV is reduced by waiting and checking the RREP packets from all the neighboring nodes to find a secure route.

4.3 Sequence number based black hole attack mitigation

In a network using AODV, sending of packets from a source node occurs by initiating a RREQ packet to its neighboring nodes in search of a best route to destination. The neighboring nodes forwards the packet further to other intermediate nodes until a best route is found. Once the destination node is found, it replies with RREP packet. There may be different route to destination. So, to determine the best route to destination, AODV considers

highest destination sequence number received from reply packet. If in this network, there is a black hole node presence, then whenever it receives the RREQ packet, it can send a counterfeit RREP packet with highest sequence number to the source node. Now, the source node ignores all other routes and chooses this route to be the best path to destination and starts sending data. The black hole node receives data and drops them without forwarding them to further nodes.

The simulation area used for this thesis is 1200 meters square. The different number of nodes (40, 60 and 80) are used assuming different nodes density scenarios and two nodes are created to act as black hole nodes. Considering the above-mentioned behavior of black hole attack, the two black hole nodes are programmed to send the largest destination sequence number upon reception of RREQ packet and drop the data packets. In other words, malicious nodes send bogus RREP packets with largest destination sequence number claiming to have a better route to destination node.

Knowing how black hole attack attracts and captures the data, the detection of a black hole presence in a network can be marked by checking the largest destination sequence number. It can be assumed that if a node can skip the node which sends largest destination sequence number then black hole attack can be prevented.

There are numerous existing approaches and schemes for black hole attack prevention in AODV. Some of those existing schemes are mentioned in the section earlier. Most of the existing schemes are complex in nature and therefore requires huge overhead and high computational power. The approach adopted for this thesis differs from those existing method in some ways. One of the contrasting differences is its simplicity. As explained previously, the approach used is exclusively based on sequence number. Therefore, it requires less computational power than other existing schemes. However, in comparison to other prevention methods, this method can only be adopted in a small to medium sized network. Despite of this limitation, its simple algorithm and effectiveness made it a better choice for this thesis work.

4. PROPOSED METHOD TO MITIGATE BLACK HOLE

To implement the prevention algorithm for this thesis, nodes are programmed to check for the destination sequence number received from RREP packet and the current sequence number in the routing table. Upon reception of RREP packet, all nodes check for the destination sequence number received from the neighboring nodes and the current sequence number in their routing table and calculates the difference between them (destination sequence number and the current sequence number). If it finds the difference between these two sequence number to be less than the predefined value (value used is 200 in this case), nodes update their routing table with the received destination sequence number and the normal AODV process is continued. But, if the difference is greater than the defined value, then the node with greater sequence number is assumed to be a black hole and is ignored and new route is searched. This is how the prevention of black hole attack is implemented for this thesis project without disturbing the traditional AODV routing method.

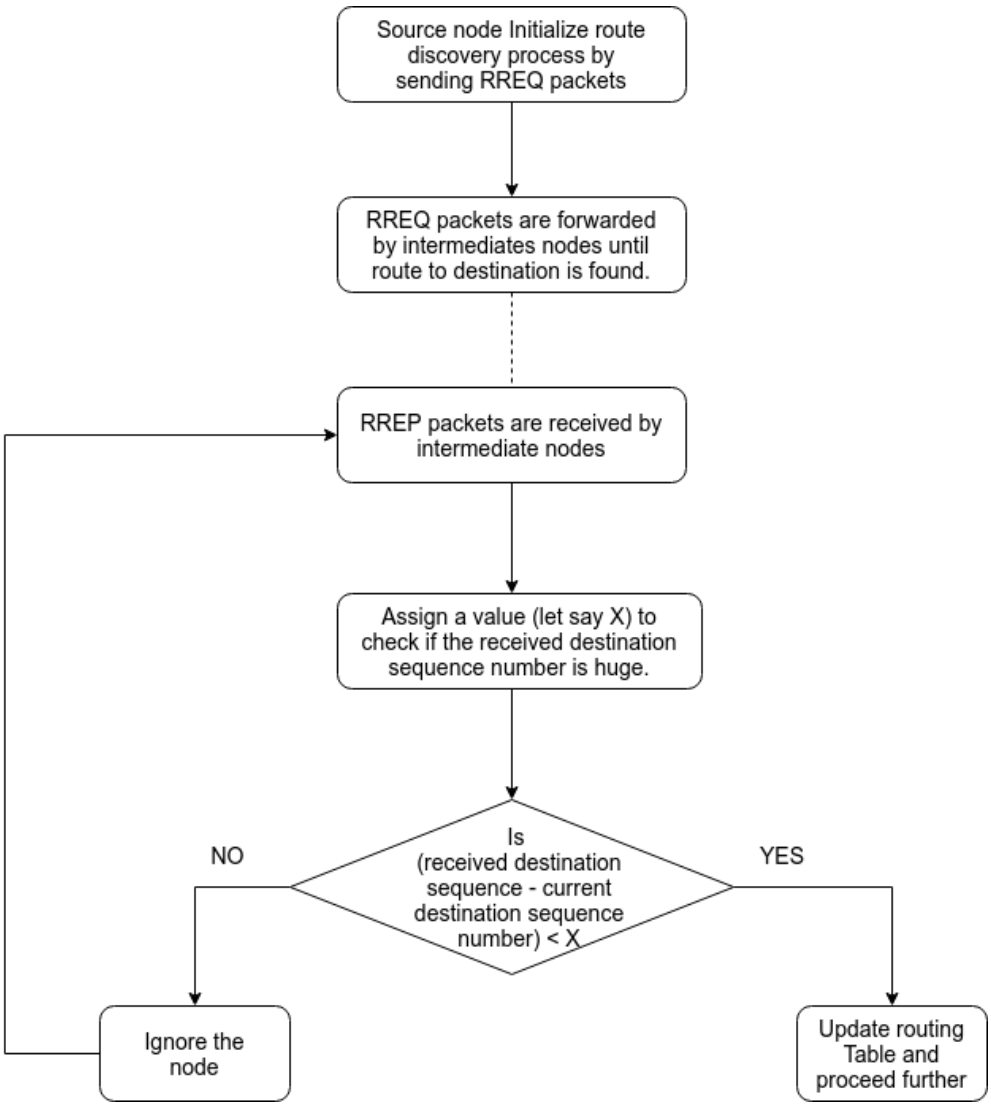

Fig. 4.2: Proposed Algorithm flowchart

The flowchart above portrays the steps of the black hole prevention method implemented in this thesis project which are briefly explained below.

Step 1: Normal AODV process take place.; source nodes initializes route discovery process by sending RREQ packets to its neighboring nodes.

Step 2: Immediate nodes upon RREQ packet reception, forwards the packet until a suitable route to destination is found.

Step 3: Once RREQ reaches to destination or a suitable route to destination is found, immediate nodes now receive RREP packet from the destination node.

Step 4: Received destination sequence number from RREP packets are checked against the current sequence number in the node's routing table. It now checks the difference between these sequence number with the assigned value X (assigned value for the simulation is 200).

Step 5: If the difference between the sequence number is greater than X:

Do not update the routing table and go to Step 3.

Else:

Update the routing table with new sequence number received from RREP.

5. IMPLEMENTATION OF BLACK HOLE ATTACK MITIGATION METHOD

This chapter of the thesis explains various simulation tools used such as SUMO, MOVE and network simulator. Apart from that, it discusses environment setups used for implementation of the black hole mitigation method. It also outlines the performance metrics used to study results obtained from the simulation.

5.1 Simulation Tools

To implement the black hole mitigation technique discussed in earlier chapter and to observe its effectiveness, it must be tested in a simulated environment. For simulation of nodes mobility, SUMO is adopted. The simulation area for the nodes used is 1200m x 1200m and different number of vehicles (40, 60 and 80) are used in different simulation. To create mobility model (vehicles, roads etc.) for the simulation in sumo, MOVE tool is used which provides users to rapidly create mobility models. Thus generated mobility models is then integration in network simulator to simulate different assumed scenarios and to produce simulation results. Further details about the tools are discussed in the sub topics below.

5.1.1 Simulation of Urban Mobility (SUMO)

Sumo is an open and free traffic simulation suite. It allows the simulation of the real-world traffic entities, such as vehicles, traffic lights, roads maps and others. According to official sumo's webpage, the features of sumo are as follows [37]:

- Microscopic simulation - vehicles, pedestrians and public transport are modeled explicitly
- Online interaction – control the simulation with TraCI
- Simulation of multimodal traffic, e.g., vehicles, public transport and pedestrians

- Time schedules of traffic lights can be imported or generated automatically by SUMO
- No artificial limitations in network size and number of simulated vehicles
- Supported import formats: OpenStreetMap, VISUM, VISSIM, NavTeq
- SUMO is implemented in C++ and uses only portable libraries

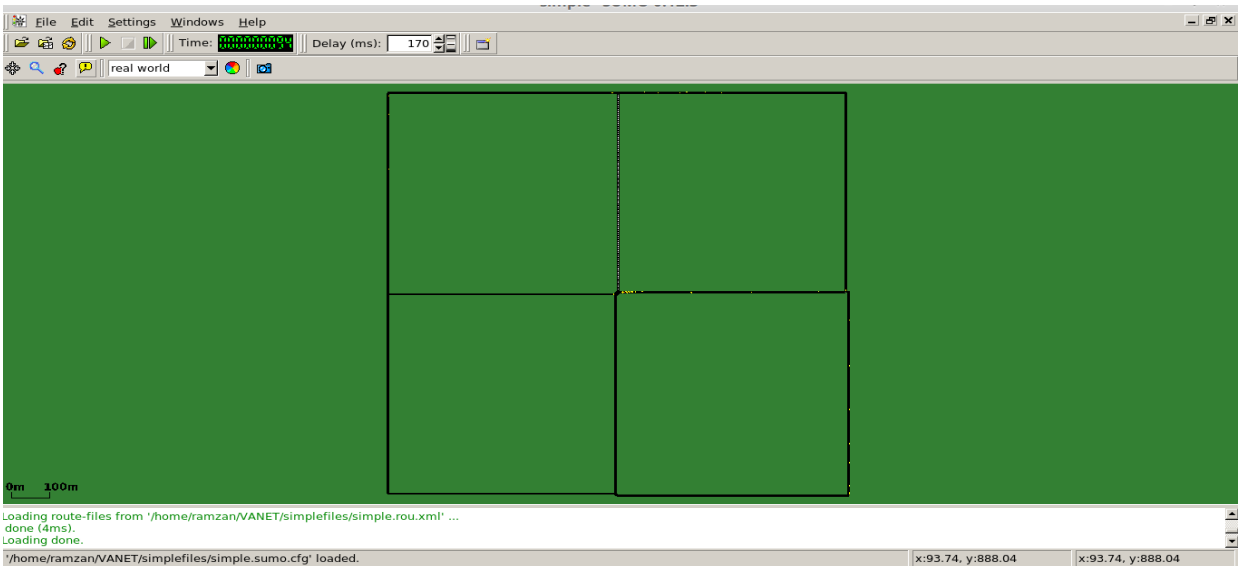

Fig. 5.1: SUMO simulation area

There are many traffic simulations tools like TraNS (Traffic and Network Simulation Environment), SUMO, STRAW, etc. which are used to generate realistic vehicular mobility. Most of these tools can be coupled with network simulator to simulate a realistic road traffics. SUMO is used in this thesis context. Figure 5.1 above and figure 5.2 below shows simulation area of vehicles in sumo.

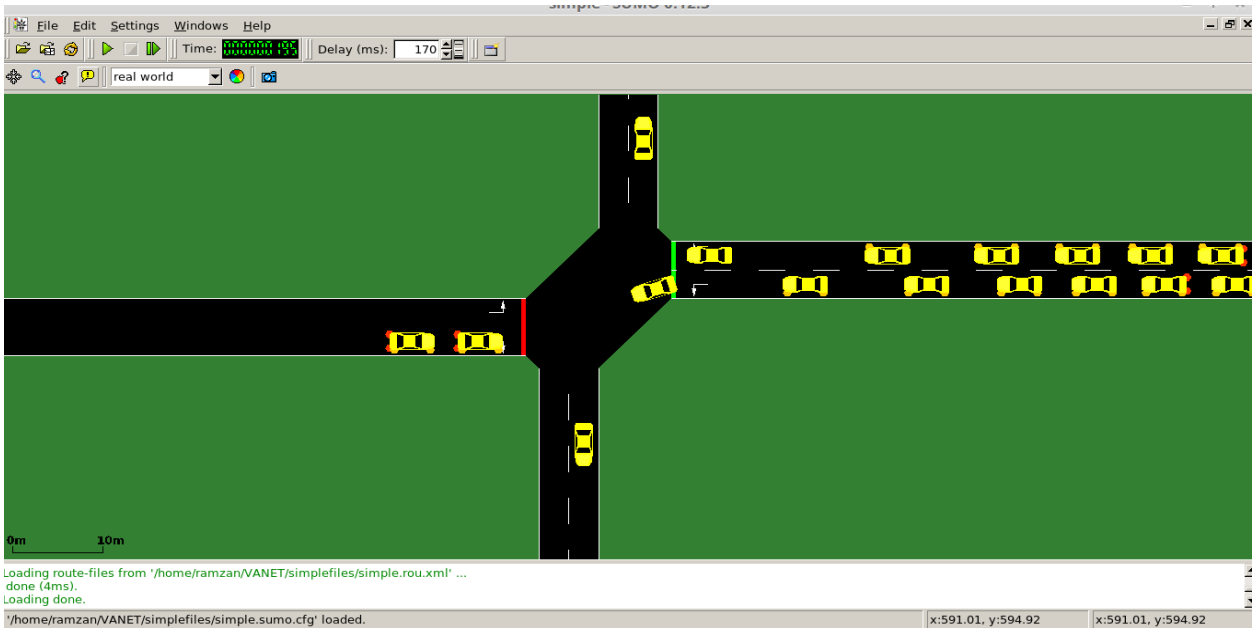

Fig. 5.2: Vehicles in sumo

This thesis deals with the vehicular network, traffic mobility is carried out using the sumo suite. For mobility model, nine nodes (junctions in sumo's context) have been created with an equidistance of 600 meters along with 12 edges with two lanes, which are shown in figures above. The nodes, edges, nodes flow, and other can be created manually using sumo alone. But MOVE tool makes it easier and quicker to generate the mobility model. Therefore, MOVE tool is adopted for the simulation for this thesis.

5.2.1 MOVE: MObility model generator for VEhicular network

It is very important to simulate and evaluate a VANET environment with various protocols in a real-world scenario. The more real a simulation gets, the immaculate a testing or evaluation gets. Most of the network simulator such as NS-3, OPNET, OMNET++, and NS-2 provides general simulation of sequence of events but they have to be customized in order to simulate VANET. Hence, in this thesis, MOVE tool is used to create real world mobility of vehicles. MOVE tool is developed on top SUMO which means that this tool facilitates the prompt mobility model generation and the scenarios creation and then integrated into SUMO environment [32].

MOVE tool is basically written in java programming language and runs on top of open source SUMO as mentioned earlier. MOVE mainly consists of two elements: Map editor and Vehicle movement editor. Using the map editor, map topology can be created manually, randomly or imported real maps from the database from freely available TIGER (Topologically Integrated Geographic Encoding and Referencing) database (US census Bureau).

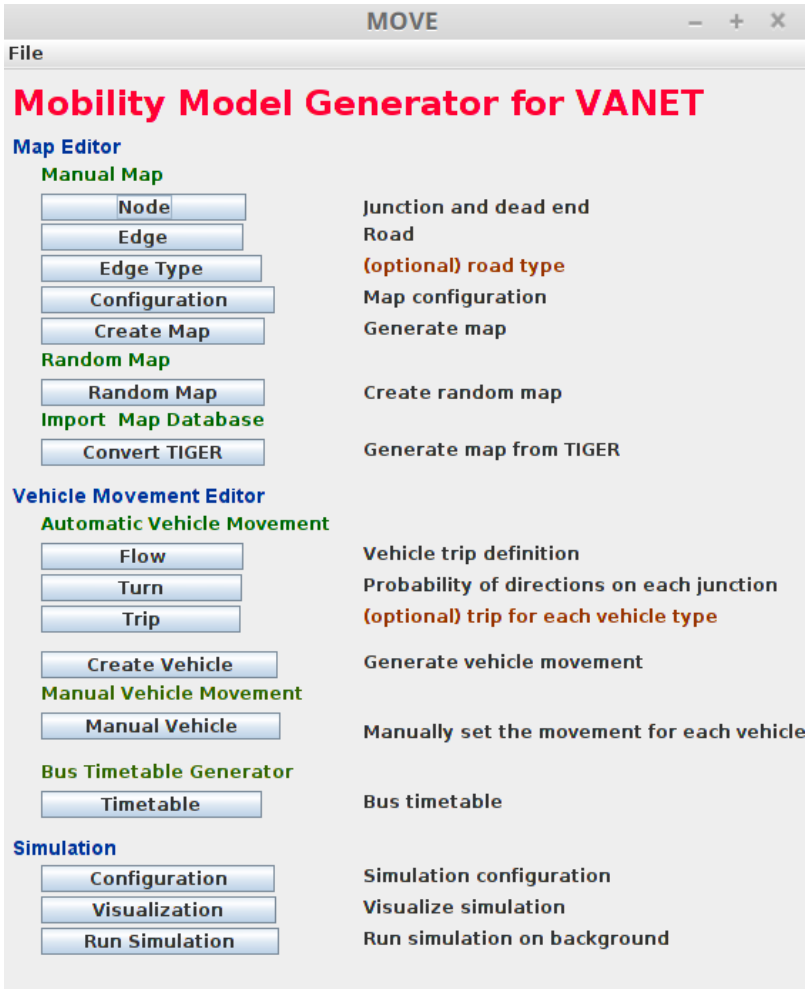

Fig. 5.3: MOVE tool

The other component i.e. Vehicle Movement editor that provides vehicles movement in the map created via Map editor. Vehicle movement can be created automatically, can be generated manually or using bus timetable generator.

The mobility model implemented for this thesis has 9 junctions and junction 1 and 5 (node0 and node5 in MOVE's context) has traffic lights. The lanes create is a two-way lane with maximum speed limit of 50 km/s except for lane number 11. Similarly, random flow of vehicles from different directions is defined using the MOVE tool. Finally, after all the necessary parameters provided to MOVE, it creates a mobility model and it is integrated in network simulator for simulation. Figure 5.4 and 5.5 shows nodes and edges created using MOVE tool.

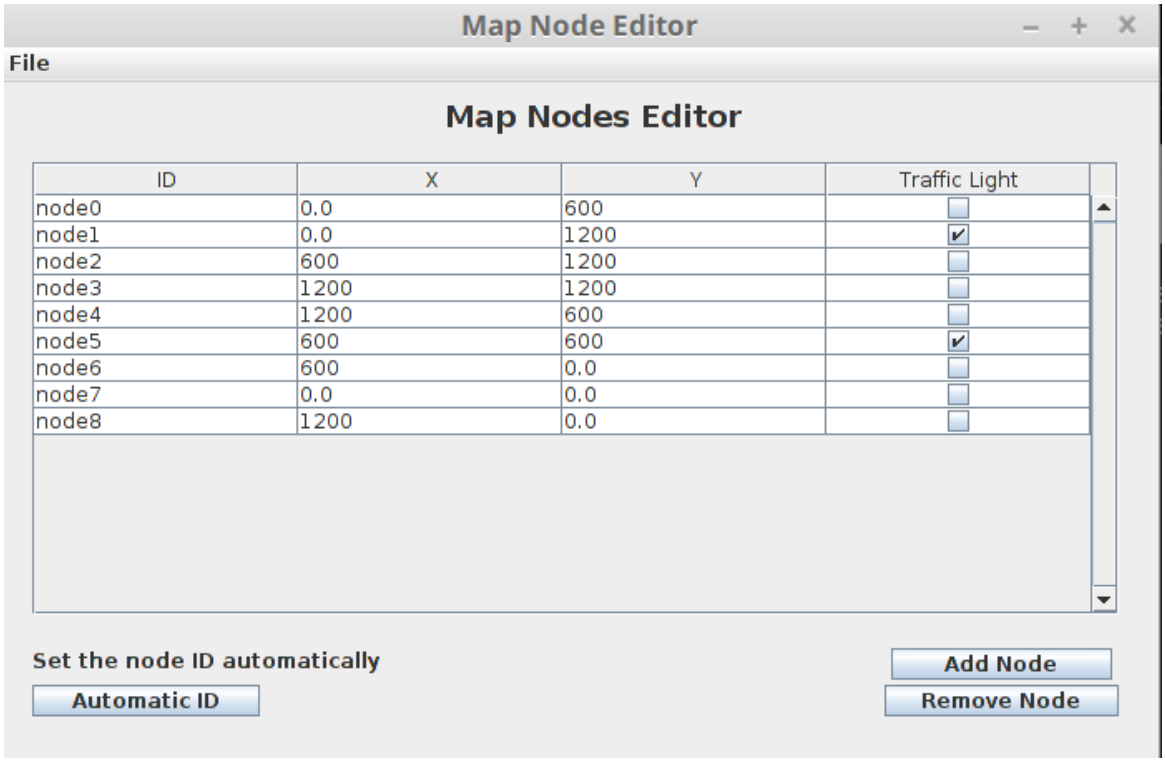

Fig. 5.4: map nodes editor in MOVE

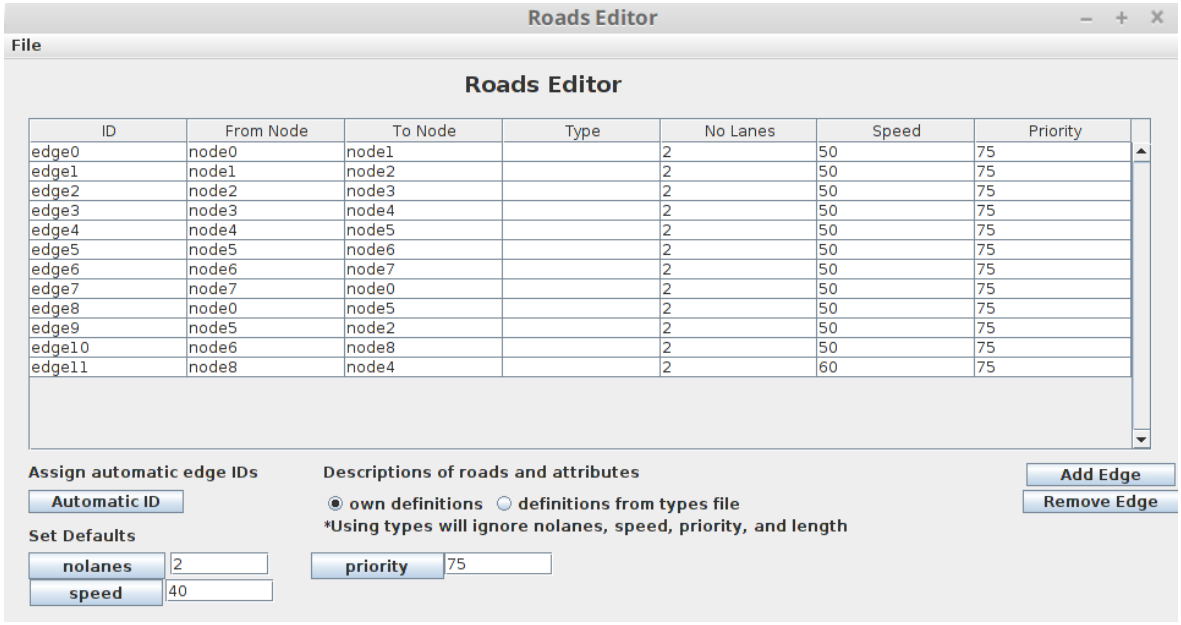

Fig. 5.5: Roads editor in MOVE

5.3.1 Network Simulator (NS)

Carrying out experimentation on various networks and system in real world can be unfeasible, impractical or expensive. Simulation of such system using simulation tool can be efficient, economical and even secure. There are many network simulation tools available for simulation of various computer networks, one of them is Network simulator (NS). It is a discrete event simulator aimed at stimulating different kinds of networks for research [35].

For this thesis project, one of the popular network simulation tools known as NS2 is used. After the completion of a simulation, NS2 generates two files with .nam and .tr extensions. NAM files are used to visualize the simulation in NS2 as shown in figures below whereas trace file (.tr) is used to analyze the simulation result. The result can then be plotted with gnuplot, xgraph or other tools. However, for this thesis project, awk scripts were used to calculate average throughput, average end-to-end delay and packet delivery ratio. Thus, obtained data was then plotted using LibreOffice Calc.

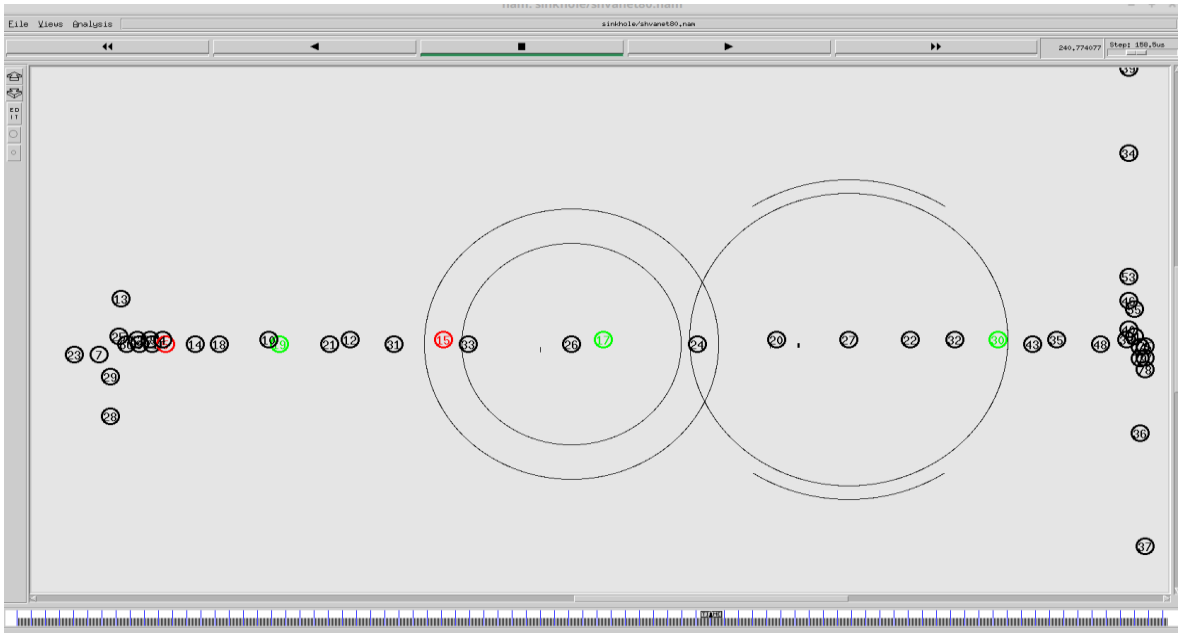

Fig. 5.6: NS2 simulation

The black nodes seen in the figures are normal nodes, green nodes represent sender and receiver nodes whereas red nodes are black hole nodes.

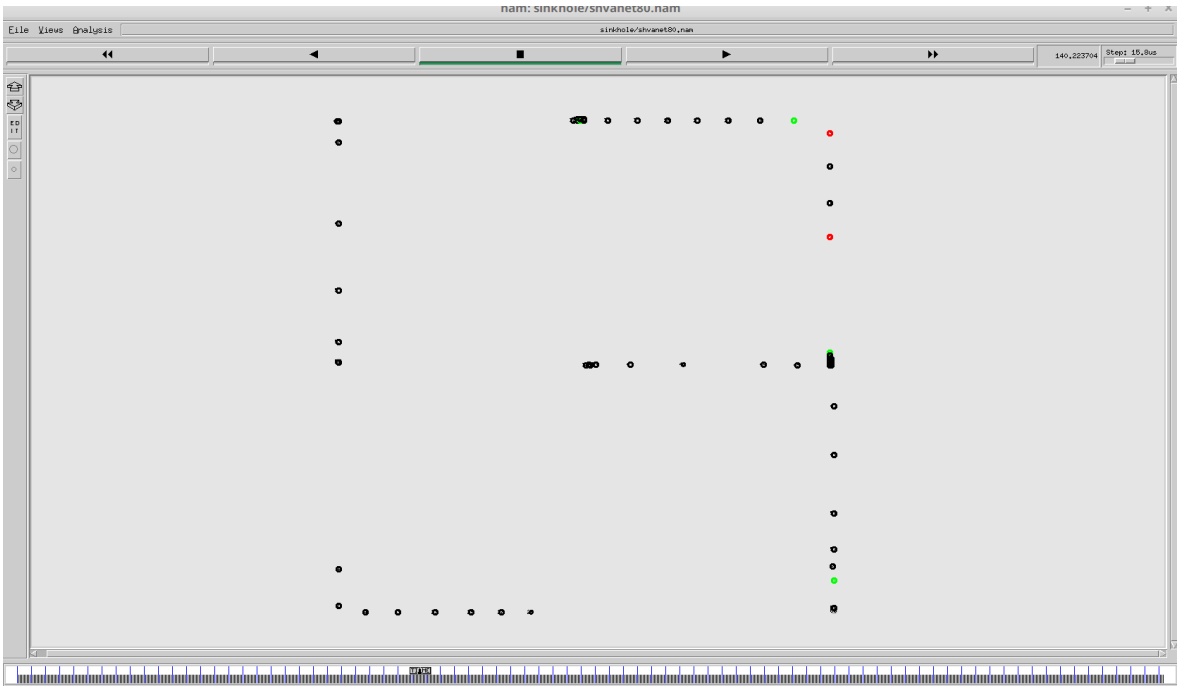

Fig. 5.7: nodes moving in ns2

The primary goal of this thesis is to understand and analyze black hole attack on AODV routing protocol and provide an approach to mitigate it. To achieve the primary goal, various scenarios have been assumed for simulation. As explained earlier, the simulation consists of different number of nodes (40, 60 and 80) in each scenario including two black hole nodes. In first scenario, the VANET simulated with different number of nodes (40, 60 and 80) without including any black hole nodes. In second scenario, two of the vehicles in ns2 were modified as black hole node and inserted in the simulation with other normal nodes. In each simulation, the number of nodes were differed except for the two black hole nodes. The effects of black hole nodes on 40, 60 and 80 nodes are evaluated. Similarly, in the last scenario, AODV was modified to use the mitigation method and the simulation was carried out with different number of nodes. Using the modified AODV, the two black hole nodes and varying number of nodes, the output of the simulation was evaluated. There were many parameters such as channel type, propagation model, network interface type, etc. were used which are discussed in next section.

5.5 Simulation environment and setup

The simulation of the VANET scenarios are implemented in NS-2.35. The topological area for the scenarios is 1200 meter by 1200 meters. The propagation model used was TwoRayGround whereas the network interface type used was wirelessPhy. TCP (Transmission Control Protocol) traffics was used to send data from source to destination nodes. Two nodes were used as source nodes and two as destination nodes. The simulation was done for 400 seconds of the simulation time.

Simulation was conducted in different conditions. First 40, 60 and 80 vehicles were used in normal condition and their average throughput, packet delivery ratio (PDR) and end-to-end (e2e) delay were calculated. In second scenario, two malicious nodes were inserted in 40, 60 and 80 vehicles topology and their respective average throughput, PDR and e2e delay was read. Similarly, in last scenario, AODV protocol was modified to ignore the malicious nodes

(nodes with greater sequence number) and routing was performed under 40, 60 and 80 nodes and again, their respective performance metrics were taken. The detailed information about the simulation parameters used are shown in the table,

Table 5.1: simulation parameters

Parameters	**Value**
Network Simulator Version	NS 2.35
Operating System	Linux Mint 18.2 (Sonya)
Channel Type	Wireless
Propagation Model	TwoRayGround
Network interface type	WirelessPhy
Interface queue type	DropTail/PriQueue
Antenna model	OmniAntenna
Routing Protocol	AODV
Number of nodes	40,60,80
Simulation time	400s
Simulation Area	1200m X 1200m
Traffic type	TCP
Maximum node speed	60km/hr.

5.4 Performance metric

The performance of a network can be determined by various metrics such as packet delay, average throughput, loss, error, bandwidth, etc. Based on these metrics, robustness and reliability of a network can analyzed. To analyze the network performance in this thesis, three metrics are used which are described below.

Average throughput: is a measure of aggregated amount of data that are transmitted in a given time. Let say, $P_{received}$ is the amount of received packets in total time T, then average throughput is calculated as

$$throughput_{average} = \frac{P_{received}}{T} \times \frac{8}{1000}$$

Average End-to-end Delay: It is the average time taken by a packet to travel from source to destination in a network. Let's assume, P_{total} is the total number of packets sent from source node at time T_{sent} and $T_{received}$ be the time taken for a packet to reach destination node. Hence Delay D is calculated as follows:

$$D = T_{received} - T_{sent}$$

If D_{total} be the total delay. An average end-to-end is a total delay divided by total number of packets sent from source to destination.

$$D_{average} = \frac{\sum D}{P_{total}}$$

Packet Delivery Ratio (PDR): is a ratio of the total number of sent packets by a source node to the total received packets by a destination node. Let say if P_{sent} be the total packet sent by source and $P_{received}$ be the total packets received by destination node, then PDR is calculated as:

$$PDR = \frac{P_{sent}}{P_{received}}$$

6. RESULT ANALYSIS

This section describes the results obtained from the simulations. The results include the network performance of AODV in different scenarios mentioned in earlier chapters. Thus obtained results are then used for analyzing the performance calculation and to show how AODV routing protocol is affected under black hole attack and after implementing the proposed algorithm. The calculation also depicts the use and limitations of the prevention method implemented.

6.1 Results for AODV (without black hole)

The table 6.1 and the figure 6.1 below depicts the network performance of AODV in normal condition (without black hole). The result suggests that the average throughput is decreasing with the increase in number of nodes whereas the packet delivery ratio seems to increase slightly with the increase in number of nodes. When 60 nodes were used, the end-to-end delay was slightly increased. But there is a rapid increase in end-to-end delay when 80 nodes were placed.

Table 6.1: AODV in normal condition

Number of nodes	Average throughput	Packet delivery Ratio	End-to-end delay
40	395.39	98.00	219.14
60	384.53	98.20	219.34
80	331.60	98.30	251.78

The network performance of AODV is shown as a graph below.

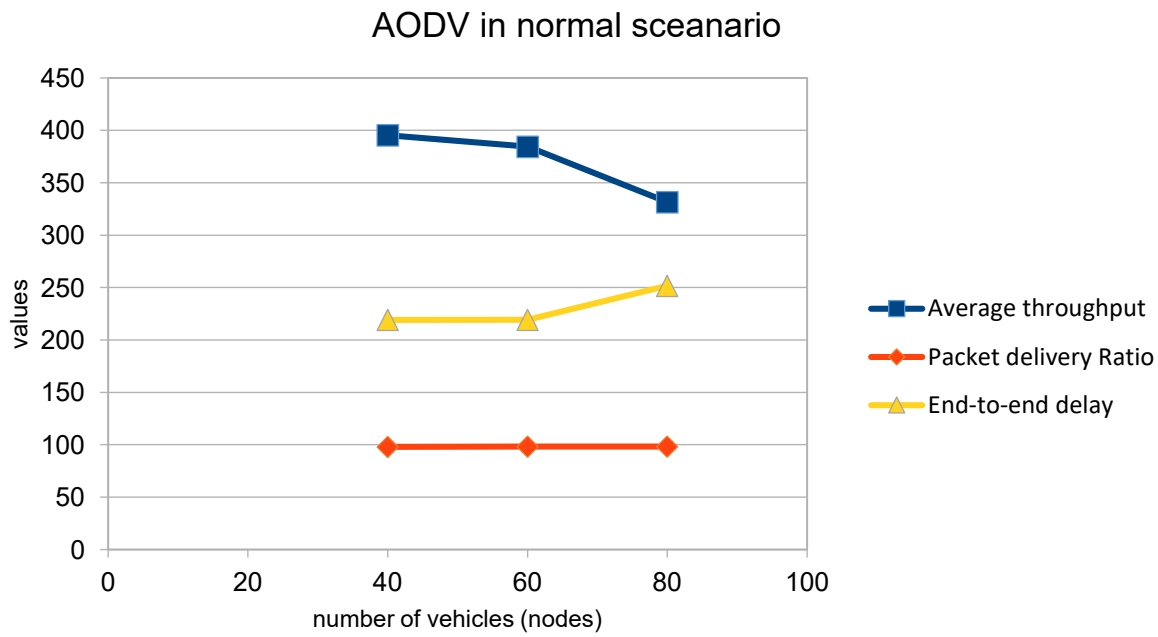

Fig. 6.1: performance of AODV

6.2 Results for AODV under black hole attack

The table 6.2 shows the performance of AODV under black hole attack. The table shows that the average throughput of AODV has decreased drastically under black hole in comparison to normal condition (without black hole). The average throughput further decreases with the increase in number of nodes. Similarly, the packet delivery ratio has also decreased with the increase in nodes under attack. As for end-to-end delay, when 40 nodes were used, the end-to-end delay was approx. 236 milliseconds (ms), the delay is decreased to 222 ms when 60 nodes were used. Again when 80 nodes were used, the delay increased to 273ms.

Table 6.2: Result for AODV under black hole

Number of nodes	Average throughput	Packet delivery Ratio	End-to-end delay
40	244.12	96.50	236.03
60	234.06	96.80	221.90
80	191.91	95.47	272.50

Similarly, the graph for AODV under a black hole attack is plotted from the table above.

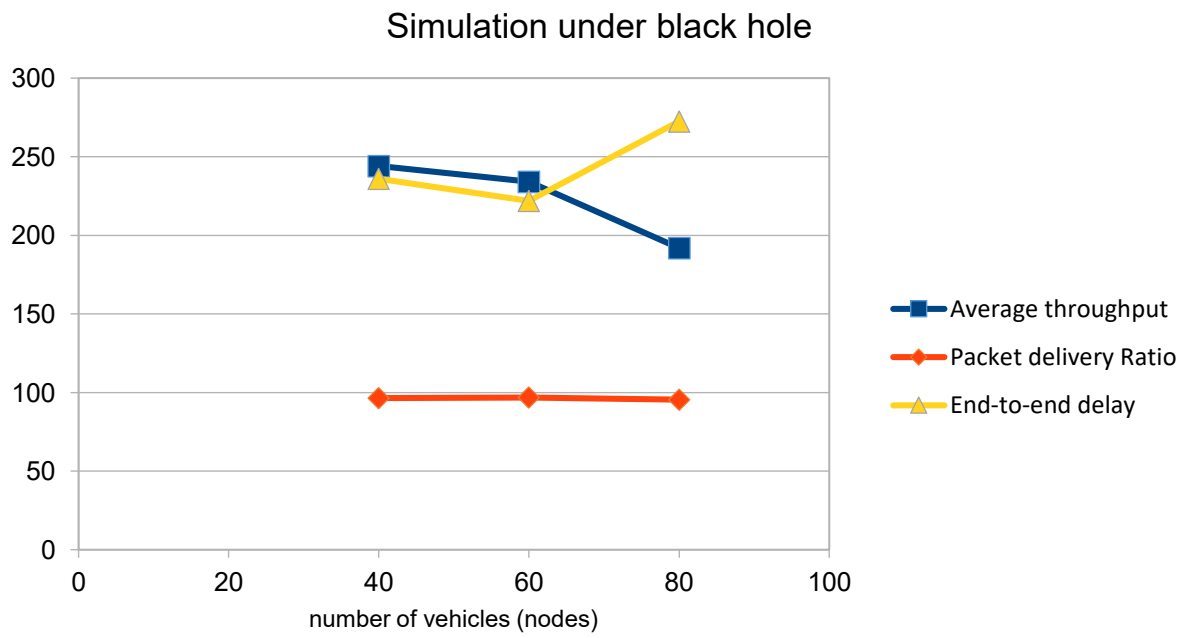

Fig. 6.2: Graph for AODV under black hole

6.3 Result for AODV with the mitigation method

After the simulation of AODV under black hole attack, AODV was modified to use the proposed algorithm. Table 6.3 shown below shows the results obtained from the simulation after modifying AODV. From the result, it is seen that when 40 nodes were used, average

throughput of modified AODV was approx. 232 Kbps. The average throughput increases to 319 Kbps (approx.) with 60 nodes and 263 Kbps (approx.) with 80 nodes. The packet delivery ratio for 40 nodes is around 97 percent. With increase in nodes number to 60, the packet delivery ratio drops to 96.5 but again increases to 98.1 percent with increase in node number i.e. 80. Similarly, the end-to-end delay for 40 and 60 nodes is 224 ms (approx.) and 222 ms (approx.). But the delay increases to 257 ms (approx.) when 80 nodes were used.

Table 6.3: Result for AODV with proposed method

Number of nodes	Average throughput	Packet delivery Ratio	End-to-end delay
40	232.41	97.20	224.20
60	318.90	96.50	221.94
80	262.70	98.16	256.52

The graph of the result obtained is shown in the figure below.

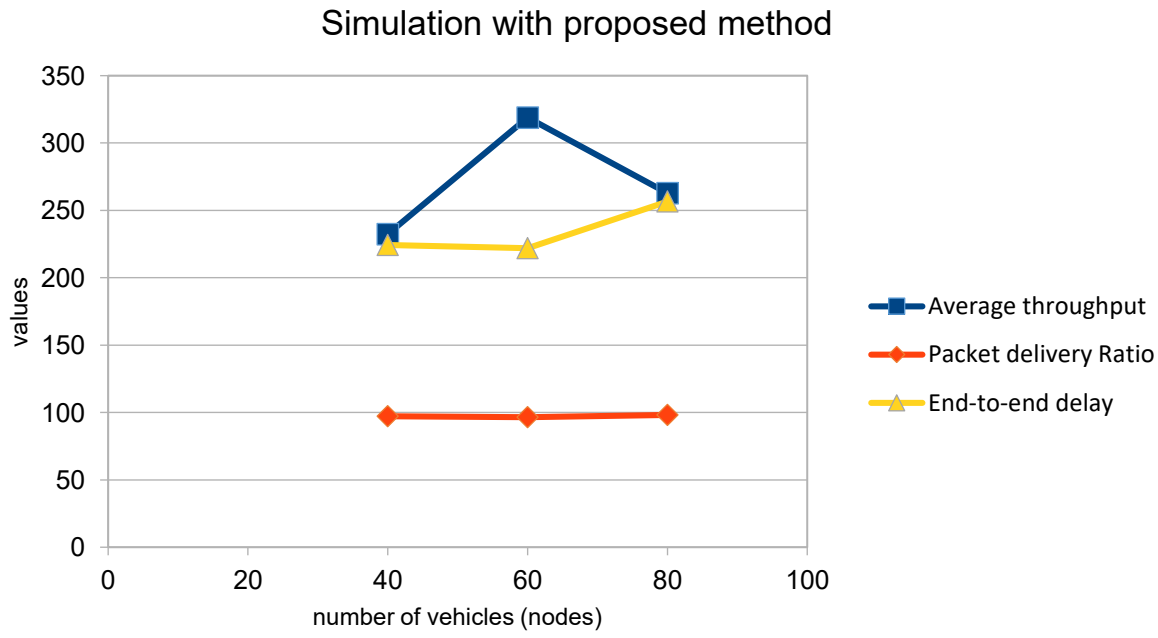

Fig. 6.3: AODV with proposed method

6.4 Discussion and Analysis

The results obtained from the simulations have provided important information about the black hole attack and what negative consequences it has on the performance of AODV routing protocol. The simulation data is further compared based on the performance metrics as shown below.

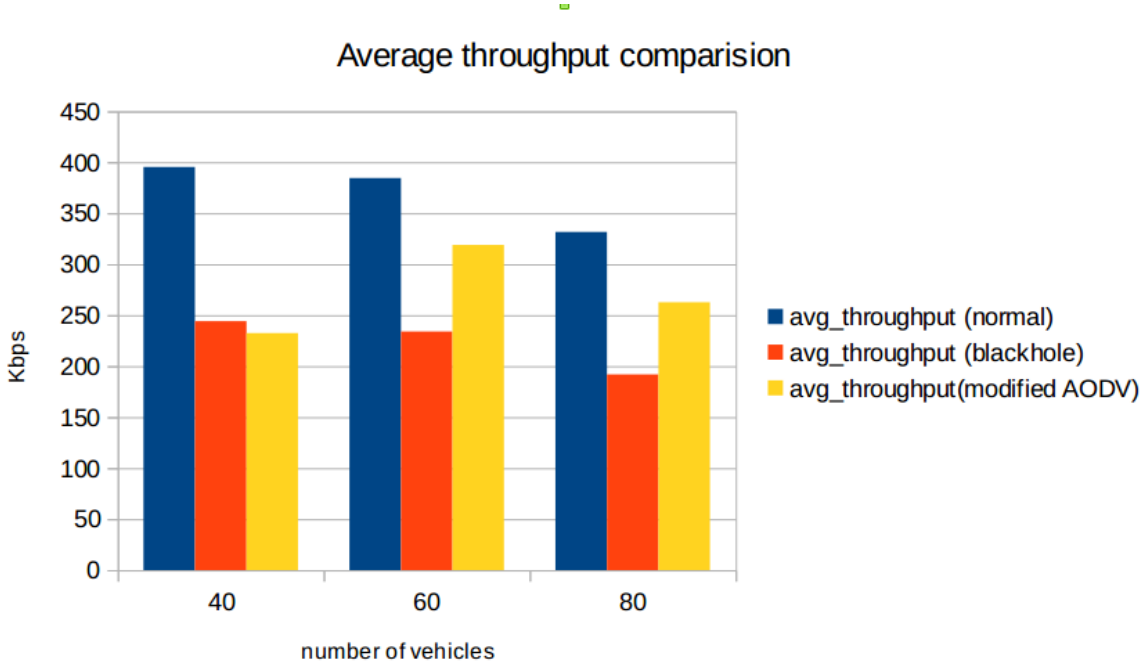

Fig. 6.4: average throughput comparison

The figure 6.4 illustrates the average throughput of AODV in different scenarios. The average throughput of AODV under black hole attack is significantly decreased. With the increase in number of nodes or vehicles, the average throughput has dropped down under black hole. From the result, it can be interpreted that the proposed method used has provided better average throughput when the network size increases. However, in case of 40 nodes, the average throughput for AODV with the mitigation approach has decreased compared to the average throughput under blackhole attack (and without mitigation method). This unexpected result can be inferred to be because of the random movement of nodes (configured via sumo) in NS2 and the nodes proximity in the simulation area. Under this scenario, when 40 nodes were used in a simulation area of 1200 m^2, the nodes could have

been out of range or signal strength could have been weak at that instance because of a smaller number of nodes moving randomly than in other scenarios (i.e. 60 and 80 nodes).

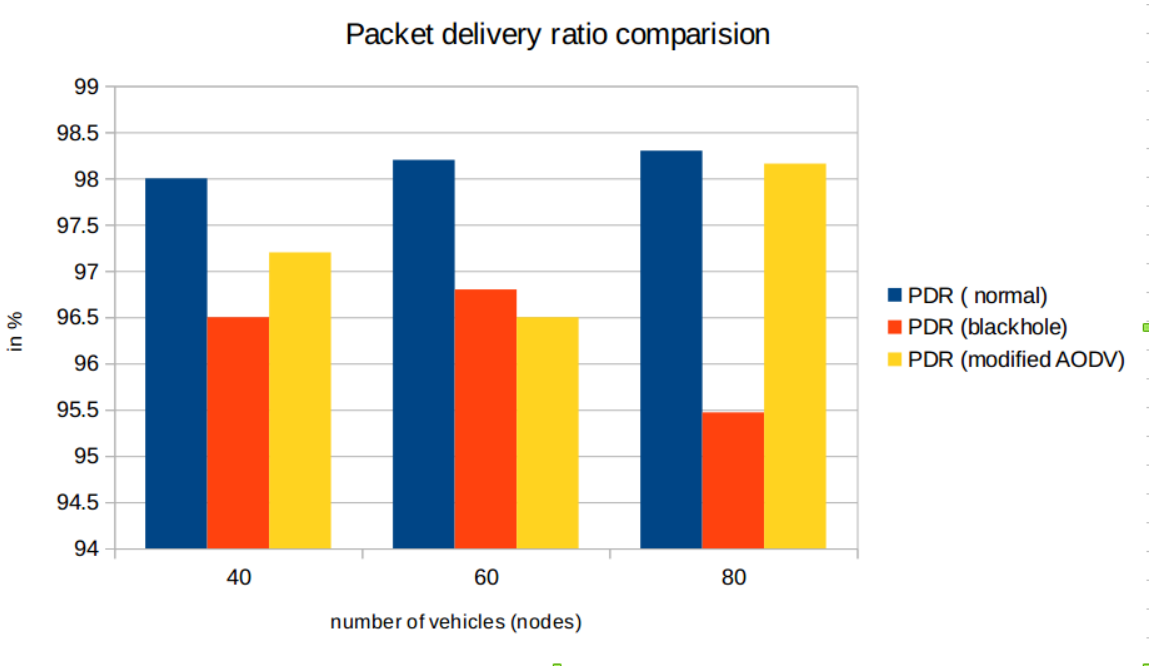

Fig. 6.5: packet delivery ratio comparison

Figure 6.5 represents the packet delivery ratio of AODV in different scenarios. The figure shows that packet delivery ratio of the AODV with proposed algorithm (modified AODV) has better ratio for 40 and 80 nodes. However, for 60 nodes, the packet delivery ratio (PDR) seems to have decreased slightly when mitigation method was used in comparison to blackhole attack (without mitigation method). There are many variables that can affect PDR. In this case, the speed and node movement may have caused constant change of signal range and possibly link, or signal breakdown could have caused, eventually reducing throughput. Generally, throughput is directly proportional to PDR and it is also reduced in this case.

As for end-to-end delay is concerned, figure 6.6 shows that the delay has improved when AODV is modified with proposed algorithm.

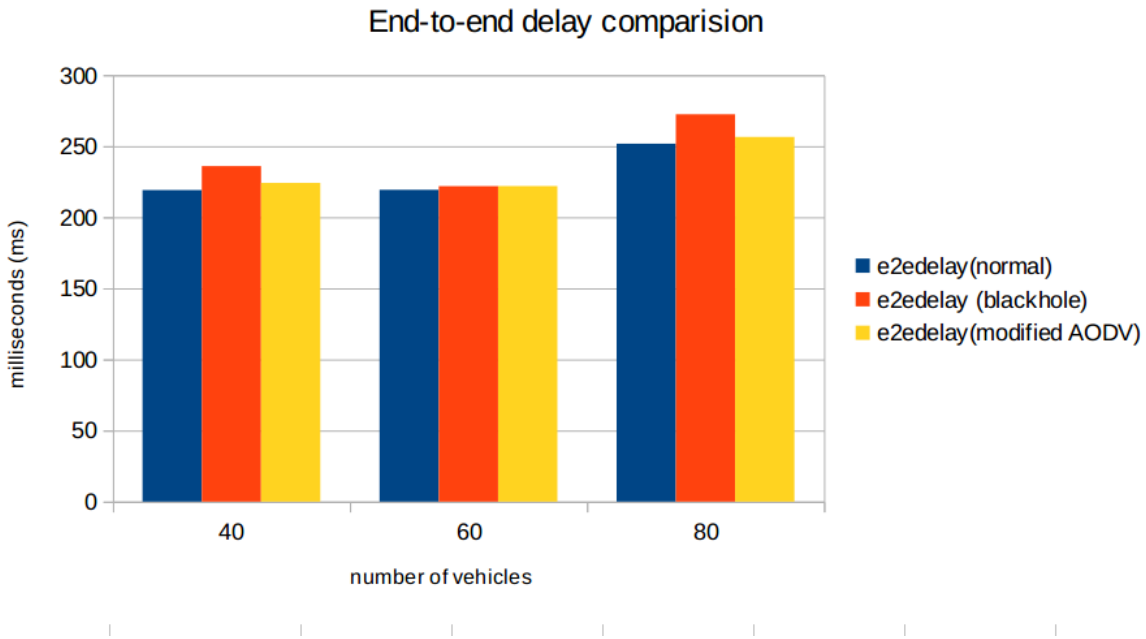

Fig. 6.6: end to end delay comparison

Analyzing all the bar graphs, it can be assumed that the modified AODV with the proposed algorithm has overall produced better results, but the results are always less than the AODV in normal situation. The reason for this could be the extra computation, AODV has to perform to check for the sequence number.

6.5 Limitations of proposed method

The proposed algorithm for this thesis works by preventing or ignoring the unanticipated huge sequence number (destination) received via RREP packet. This method is limited to ignoring black hole attacks only which sends large destination sequence number to establish a route towards itself. This method lacks the black hole identification and authentication of

all the nodes in the network. Despite of proposed method implementation, the black hole attacker nodes are still receiving RREQ packets from the neighbors and hence their threats are not eradicated completely.

The method for preventing black hole attack in this thesis checks for the source and destination sequence number and if the difference is greater than 100, it is a black hole and therefore, the routing table is not updated. In other words, only the nodes with the sequence number difference of less than 100 can take part in routing process. In a huge network with huge number of nodes, using this approach may not be able to mitigate the attacker nodes completely. Hence, the proposed method has a limited application and scope to a smaller network. Apart from these, the proposed method does not have a capacity to detect other form of attacks.

7. CONCLUSION

An insecure VANET system can lead to serious injuries, fatal accidents and even deaths. Therefore, VANET system must be highly secure and robust and be capable of preventing possible danger that can occur because of security failure. This thesis reviews the routing protocols that can be used in VANET, the possible threats on those protocols and the available counter-measures to those threats.

This thesis demonstrates the emphasis of security aspect of routing protocols by using AODV routing protocol and the effects it can have on performance of AODV routing protocol when black hole attack is launched. It also discusses the counter-measures for black hole attack and illustrates a simple sequence number based black hole prevention method. In order to achieve the objective of this thesis, the simulation was performed in network simulator and other mobility tools. Various scenarios were assumed with different number of nodes and the simulation data was evaluated. Upon analyzing the results collected from the simulation, it shows that the black hole attack can have negative impact on the network performance. The average throughput and packet delivery ratio decreased under black hole attack and the end-to-end delay was increased.

The result from the simulation shows that the overall average throughput and average packet delivery ratio of AODV in all scenarios (under black hole attack) were 223,69 kbps (approx..) and 0.963 (approx..) respectively. When the prevention algorithm was implemented, the aggregate average throughput and average packet delivery ratio of AODV were increased to 271,33 kbps and 0.972 (approx..). Therefore, it can be said that the prevention method was able to increase the average throughput of AODV by remarkable 21,3% in comparison with black hole attack without prevention method.

The approach implemented to mitigate black hole was able to prevent effects of black hole attack and better the overall performance of AODV routing protocol especially average throughput to a convincing amount. Although the prevention method increased the overall AODV performance against black hole, this method was not able to perform as in the normal scenario. Apart from this, this method will be inefficient if the difference between the

destination sequence number and the current sequence number is too large. Hence, it is limited to a small to medium sized network. Finally, it can be concluded that for a better network performance, a secure protocol plays a significant role. A routing protocols for VANET must be immune from various attacks for a smooth, secure and safe traffic condition. Hence, security of routing protocols in VANET is very important.

References

1) Basagni, S., Conti, M., Giordano, S. and Stojmenovic, I. (2004). *Mobile ad hoc networking*. Hoboken, N.J.: John Wiley.

2) Corson, S. and Macker, J. (1999). [online] Tools.ietf.org. Available at: https://tools.ietf.org/pdf/rfc2501.pdf

3) Campolo, C., Molinaro, A. and Scopigno, R. (n.d.). Vehicular ad hoc Networks. Springer International Publishing.

4) Kaur, M., Kaur, S. and Singh, G. (2012). *VEHICULAR AD HOC NETWORKS*. [online] Rroij.com. Available at: http://www.rroij.com/open-access/vehicular-ad-hoc-networks-61-64.pdf

5) Yousefi, S., Mousavi, M. and Fathy, M. (2006). Vehicular Ad hoc Networks (VANETs): challenges and perspectives. Available at: https://ieeexplore.ieee.org/document/4068700.

6) B G, P., Miller, J., R, S. and RAM, R. (2016). A Review of Security Threats, Solutions and Trust Management in VANETs. [online] Available at: https://www.researchgate.net/publication/306400368_A_Review_of_Security_Threats_Solutions_and_Trust_Management_in_VANETs

7) Hartenstein, H. and Laberteaux, K. (2008). A tutorial survey on vehicular ad hoc networks. IEEE Communications Magazine, 46(6)

8) IEEE Draft Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture. (2012). pp.164-171.

9) Rajkumar, N., Nithya, M. and HemaLatha, P. (2016). *OVERVIEW OF VANET WITH ITS FEATURES AND SECURITY ATTACKS*. [online] Irjet.net. Available at: https://www.irjet.net/archives/V3/i1/IRJET-V3I124.pdf

10) 1609.2-2013 IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages. (n.d.).

11) Perkins, C., Belding-Royer, E. and Das, S. (2003). Ad hoc On-Demand Distance Vector (AODV) Routing. [online] rfceditor.org. Available at: https://www.rfceditor.org/rfc/pdfrfc/rfc3561.txt.pdf

12) Ahmed, S., Ariffin, S. and Fisal, N. (2013). Overview of Wireless Access in Vehicular Environment (WAVE) Protocols and Standards. Indian Journal of Science and Technology, pp.4494-4499.

13) Zhou, Y., Wu, D. and Nettles, S. (2004). Analyzing and Preventing MAC-Layer Denial of Service Attacks for Stock 802.11 Systems. [online] Broadnets.org. Available at: http://broadnets.org/2004/workshop-papers/Broadwise/Zhou_Y.pdf

14) Li, Y. (2010). *An Overview of the DSRC/WAVE Technology*. Available at: https://link.springer.com/chapter/10.1007/978-3-642-29222-4_38.

15) Frank, R., Sommer, C., Kargl, F., Dietzel, S. and Van der Heijden, R. (n.d.). (Anon., ei pvm)(FG-IVC 2015). Ulm, Germany, pp.5-6.

16) Li, M. (2014). Security in VANETs. [online] Cse.wustl.edu. Available at: https://www.cse.wustl.edu/~jain/cse571-14/ftp/vanet_security.pdf

17) Singh, S. and Agrawal, S. (2014). *VANET routing protocols: Issues and challenges - IEEE Conference Publication*. [online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/abstract/document/6799625

18) Gilles Engoulou, R., Bellaïche, M., Pierre,, S. and Quintero, A. (2014). VANET security surveys. [online] Mocom.xmu.edu.cn. Available at: http://mocom.xmu.edu.cn/home/project/vanet/1%20Survey/6%20VANET%20security%20surveys.pdf

19) Singh, V. and Kumar, S. (2016). Black Hole Detection in MANET Using Modified AODV Protocol. [online] Ijircce.com. Available at: http://www.ijircce.com/upload/2016/february/108_BLACK.pdf

20) Suryawanshi, R. and P M, V. (2012). Analysis and Prevention of Black Hole Attack in Ad-Hoc Networks. [online] Ijcst.com. Available at: http://ijcst.com/vol34/4/ranjeet.pdf

21) Mokhtar, B. and Azab, M. (2019). Survey on Security Issues in Vehicular Ad Hoc Networks. Alexandria Engineering Journal (2015) 54, 1115–1126. [online] Available at: http://www.elsevier.com/locate/aej.

22) Raj, C., Upadhayaya, U., Makwana, T. and Mahida, P. (2014). Simulation of VANET Using NS-3 and SUMO. [online] Pdfs.semanticscholar.org. Available at: https://pdfs.semanticscholar.org/9f15/f7498ac65bbf3d3ff7934e739dc5ce8697c9.pdf

23) Rehmani, M., Doria, S. and Senouci, M. (2010). A Tutorial on the Implementation of Ad-hoc On Demand Distance Vector (AODV) Protocol in Network Simulator (NS-2). [online] Available at: https://arxiv.org/abs/1007.4065

24) Samatha, B., Kumar, D. and Karyemsetty, N. (2019). Design and Simulation of Vehicular Ad-hoc Network using SUMO and NS2. [online] Ripublication.com. Available at: https://www.ripublication.com/awmc17/awmcv10n5_31.pdf

25) Khairnar, V. and Pradhan, D. (2010). Mobility Models for Vehicular Ad-hoc Network Simulation. International Journal of Computer Applications, 11(4), pp.8-12.

26) Census.gov. (2019). TIGER Products - Geography - U.S. Census Bureau. [online] Available at: https://www.census.gov/geo/maps-data/data/tiger.html

27) Varshney, T. (2019). Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network - IEEE Conference Publication. [online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6821389

28) Nadeem, A. and Howarth, M. (2019). A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks - IEEE Journals & Magazine.

[online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/document/6489880

29) Thachil, F. and Shet, K. (2019). A Trust Based Approach for AODV Protocol to Mitigate Black Hole Attack in MANET - IEEE Conference Publication. [online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/document/6391690

30) Moudni, H., Er-Rouidi, M., Mouncif, H. and El Hadadi, B. (2016). Attacks against AODV Routing Protocol in Mobile Ad-Hoc Networks - IEEE Conference Publication. [online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/document/7467743

31) Tamilselvan, L. and Sankaranarayanan, V. (2007). Prevention of Black hole Attack in MANET - IEEE Conference Publication. [online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/abstract/document/4299670 [Accessed 15 Dec. 2018].

32) Karnadi, F., Mo, Z. and Lan, K. (2019). MOVE: A MObility model generator for VEhicular network. [online] Csie.ncku.edu.tw. Available at: http://www.csie.ncku.edu.tw/~klan/data/materials/mobicom2005.pdf

33) Ahmed, M. and Hussain, M. (2014). Performance of an IDS in an Ad-hoc Network under Black Hole and Gray Hole attacks - IEEE Conference Publication. [online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/document/6767377

34) Jalil, K., Ahmad, Z. and Ab Manan, J. (2019). ERDA: Enhanced Route Discovery Mechanism for AODV Routing Protocol against Black Hole Attacks. [online] Pdfs.semanticscholar.org. Available at: https://pdfs.semanticscholar.org/8a6c/f25396429dd34752c09019b42c49fb69aab1.pdf

35) Isi.edu. (n.d.). Marc Greis' Tutorial for the UCB/LBNL/VINT Network Simulator "ns". [online] Available at: https://www.isi.edu/nsnam/ns/tutorial/

36) Pattberg, B. (n.d.). *DLR - Institute of Transportation Systems - SUMO – Simulation of Urban MObility*. [online] Dlr.de. Available at: https://www.dlr.de/ts/en/desktopdefault.aspx/tabid-9883/16931_read-41000/

APPENDIX

```
#
# ======================================================================
# Define options
#
# ======================================================================
set val(chan)   Channel/WirelessChannel                    ;# channel type
set val(prop)   Propagation/TwoRayGround                   ;# radio-propagation model
set val(netif)  Phy/WirelessPhy                ;# network interface type
set val(mac)    Mac/802_11                     ;# MAC type
set val(ifq)    Queue/DropTail/PriQueue             ;# interface queue type
set val(ll)     LL                  ;# link layer type
set val(ant)    Antenna/OmniAntenna                ;# antenna model
set val(ifqlen) 50                  ;# max packet in ifq
set val(nn)     96          ;# number of mobilenodes
set val(rp)     AODV                       ;# routing protocol

set opt(x)      1252                       ;# x coordinate of topology
set opt(y)      1252                      ;# y coordinate of topology
set stopTime      199.00

#
# ======================================================================
# Main Program
#
# ======================================================================
#
# Initialize Global Variables
#
set ns_ [new Simulator]
set tracefd [open /home/ramzan/VANET/simpleBHprev.tr w]
$ns_ trace-all $tracefd

set namtrace [open /home/ramzan/VANET/simpleBHprev.nam w]
$ns_ namtrace-all-wireless $namtrace $opt(x) $opt(y)

# set up topography object
set topo    [new Topography]
$topo load_flatgrid $opt(x) $opt(y)

#
# Create God
#
```

```
create-god $val(nn)

# Configure node

set chan_1_ [new $val(chan)]
$ns_ node-config  -ad-hocRouting $val(rp) \
                  -llType $val(ll) \
                  -macType $val(mac) \
                  -ifqType $val(ifq) \
                  -ifqLen $val(ifqlen) \
                  -antType $val(ant) \
                  -propType $val(prop) \
                  -phyType $val(netif) \
                  -topoInstance $topo \
                  -agentTrace ON \
                  -routerTrace ON \
                  -macTrace ON \
                  -movementTrace ON \
                  -channel $chan_1_

for {set i 0} {$i < $val(nn)} {incr i} {
  set node_($i) [$ns_ node]
  $node_($i) random-motion 0 ;# disable random motion
}

# nodes colors
$node_(10) color "red"
$ns_ at 0.1 "$node_(10) color red"
$node_(12) color "red"
$ns_ at 0.1 "$node_(12) color red"
$node_(4) color green”
$ns_ at 0.1 "$node_(4) color green "
$node_(2) color green
$ns_ at 0.1 "$node_(2) color green "
$node_(16) color green”
$ns_ at 0.1 "$node_(16) color green "
$node_(8) color green
$ns_ at 0.1 "$node_(8) color green "




#
# Provide initial (X,Y, for now Z=0) co-ordinates for mobilenodes
#
#predefine node in NAM
  # ID of SUMO: flow0_0
$node_(0) set X_ 19.95
```

```
$node_(0) set Y_ 624.0500000000001
$node_(0) set Z_ 0.0
$node_(0) setdest 19.95 624.0500000000001 1
  # ID of SUMO: flow1_0
$node_(1) set X_ 1219.95
$node_(1) set Y_ 22.549999999999997
$node_(1) set Z_ 0.0
$node_(1) setdest 1219.95 22.549999999999997 1
  # ID of SUMO: flow0_1
$node_(2) set X_ 19.95
$node_(2) set Y_ 624.0500000000001
$node_(2) set Z_ 0.0
$node_(2) setdest 19.95 624.0500000000001 1
  # ID of SUMO: flow1_1
$node_(3) set X_ 1219.95
$node_(3) set Y_ 22.549999999999997
$node_(3) set Z_ 0.0
$node_(3) setdest 1219.95 22.549999999999997 1
.
.
.
.
truncated
.
.
.
$ns_ at 198.0 "$node_(43) setdest 619.95 625.5799999999999 10.32"
$ns_ at 198.0 "$node_(41) setdest 619.95 651.4799999999999 11.88"
$ns_ at 198.0 "$node_(39) setdest 619.95 680.15 14.10"
$ns_ at 198.0 "$node_(33) setdest 619.95 710.5899999999999 16.31"
$ns_ at 198.0 "$node_(31) setdest 619.95 761.55 19.88"
$ns_ at 198.0 "$node_(21) setdest 619.95 1199.44 0.09"
$ns_ at 198.0 "$node_(12) setdest 619.95 1206.9499999999998 0.00"
$ns_ at 198.0 "$node_(17) setdest 616.65 1206.94 0.00"


#black hole
$ns_ at 10.0 "[$node_(10) set ragent_] bh"
$ns_ at 10.0 "[$node_(12) set ragent_] bh"


# Setup traffic flow between nodes
Agent/TCP set window_ 20
Agent/TCP set packetSize_ 1000
Agent/TCP set maxburst_ 0
Agent/TCP set maxcwnd_ 0
Agent/UDP set packetSize_ 1000
Application/Traffic/CBR set rate_ 64Kb
```

```
Application/Traffic/CBR set random_ NO
Application/Traffic/CBR set maxpkts_ 2280000

set tcp0 [new Agent/TCP]
$tcp0 set class_ 2
set sink0 [new Agent/TCPSink]
$ns_ attach-agent $node_(2) $tcp0
$ns_ attach-agent $node_(8) $sink0
$ns_ connect $tcp0 $sink0
set ftp0 [new Application/FTP]
$ftp0 attach-agent $tcp0
$ns_ at 0.0 "$ftp0 start"

$ns_ at 200.0 "$ftp0 stop"


set tcp1 [new Agent/TCP]
$tcp1 set class_ 2
set sink1 [new Agent/TCPSink]
$ns_ attach-agent $node_(4) $tcp1
$ns_ attach-agent $node_(16) $sink1
$ns_ connect $tcp1 $sink1
set ftp1 [new Application/FTP]
$ftp1 attach-agent $tcp1
$ns_ at 0.0 "$ftp1 start"

#$ns_ at 200.0 "$ftp1 stop"

#
# Tell nodes when the simulation ends
#
for {set i 0} {$i < $val(nn) } {incr i} {
    $ns_ at $stopTime "$node_($i) reset";
}
$ns_ at $stopTime "stop"
$ns_ at $stopTime "puts \"NS EXITING...\" ; $ns_ halt"
proc stop {} {
    global ns_ tracefd namtrace
    $ns_ flush-trace
    close $tracefd
    close $namtrace
}

puts "Starting Simulation..."
$ns_ run
```