Blackhole Attack Detection In AODV Protocol On VANET

A PROJECT REPORT

Submitted By

AMINUL ISLAM TANVIN

ID No. 11509015

In partial fulfillment for the award of the degree

of

BACHELOR OF SCIENCE (ENGINEERING)

in

INFORMATION ANDCOMMUNICATION TECHNOLOGY

COMILLA UNIVERSITY :: CUMILLA-3506

MARCH 2020

COMILLA UNIVERSITY :: CUMILLA-3506

BONAFIDE CERTIFICATE

This is to certify that the project entitled, **“Blackhole Attack Detection In AODV Protocol On VANET”** and submitted by **“AMINUL ISLAM TANVIN”** in partial fulfillment of the requirements of ICT-800 Research Project and Viva embodies the work done by him under my supervision.

Md. Tofael Ahmed
CHAIRMAN, EXAM COMMITTEE
Associate Professor,
Department of Information and
Communication Technology
Comilla University, Cumilla

Md. Rakib Hasan
SUPERVISOR
Lecturer,
Department of Information and
Communication Technology
Comilla University, Cumilla

Abstract

Vehicular mobility is a very important part of the network industry. As the world changed, every wired communication replaced by wireless communication. That's why VANET is very important. For being wireless it has lots of facilities. Also, have some drawbacks about the security issue. This type of network is affected by network attack like blackhole attack. Without taking steps against this issue the vanet is not reliable. A new blackhole attack detection technique is proposed which uses AODV as routing protocol. It detects the blackhole nodes and sends the information to the admin of the network. We also compare the blackhole attack with a flawless network.

Acknowledgements

At first, I want to express gratitude to the Almighty Allah for His endless kindness for keeping me mentally and physically fit to complete this sophisticated task.

I would like to express my special thanks of gratitude to my honorable supervisor Md. Rakib Hasan, who gave me the golden opportunity to do this wonderful project on this topic. His sage advice, insightful criticisms, and patient encouragement aided the completion of this project in innumerable ways. I came to know about so many new things, I am greatly thankful to him.

I am also thankful to Head of Department, or the motivation and inspiration that triggered me for this thesis work.

I would like to express my gratitude to all the teachers in my department for building me to do this work.

Contents

List of Figures

List of Tables

List Of Abbreviations

NetAnim	**NET**work **ANIM**ator
VANET	**V**ehicular **A**d-hoc **NET**work
AODV	**A**d-hoc **O**n-Demand **D**istance **V**ector
RREQ	**R**outing **REQ**uest
SUMO	**S**imulation of **U**rban **MO**bility
NS2	**N**etwork **S**imulator **2**
IDS	**I**ntrusion **D**etection **S**ystem
IPS	**I**ntrusion **P**revention **S**ystem
OSM	**O**pen **S**treet **M**ap

Chapter 1

Introduction

Bangladesh has a very high road accident fatality rate. Every day around eight per- sons die in road accidents.[1] So road security is the main issue for now. To trade off with traffic accidents and vehicle speed we have to develop new road technology. That's why VANET is important now a day.

1.1 Introduction

A Vehicular Ad hoc Network (VANET) is a form of wireless ad-hoc network to provide communications among vehicles and nearby roadside equipment. It is emerging as a new technology to integrate the capabilities of a new generation wireless networking to vehicles. The major purpose of VANET is to provide (1) ubiquitous connectivity while on the road to mobile users, who are otherwise connected to the outside world through other networks at home or the work place, and (2) efficient vehicle-to-vehicle communications that enable the Intelligent Transportation Systems (ITS). ITS includes a variety of applications such as cooperative traffic monitoring, control of traffic flows, blind crossing (a crossing without light control), prevention of collisions, nearby information services, and real-time detour routes computation.

1.2 Motivation

Bangladesh is the 12th most densely settled nation on earth. The traffic jam is the most threat to developing countries like Bangladesh. Only Dhaka's traffic jams eat up 3.2 million working hours each day and drain billions of dollars from the city's economy annually. So it is important to develop a new international standard on the road. That is not other than VANET. When a new technology is evolved the security is the main concern. The intruder uses the technology to threaten the improvement. To improve network-level security we work for network layer attack (blackhole). This blackhole attack detection helps us to improve the infrastructure of our road and vehicle.[1]

There are not enough routes to transport the metropolis's 17 million-plus residents. For being a member of this country it is a job to think about the problem of this country and try to solve them.

1.3 Rationale of the Study

In this research, simulation of a network layer attack(blackhole) is done using NS2 as a simulator. Blackhole attack is a denial of service attack where a malicious node pretends to be the first hop for the shortest path. When the packet is sent to the blackhole node it drops the packet instead of sending the packet to the next hop. In vanet, it is hard to define a node as blackhole because many legitimate node drop packet(s) for proper reason.

VANET is a figureless topology. That's why the node(s) are not stable in one place, so the malicious node could be change location and pretend to be a legitimate node. Blackhole nodes have to be blocked by the MAC address.

1.4 Research Questions

The research questions for this study were:

1. How to Detect malicious node(s) in Blackhole attack on VANET?

2. Is this approach efficient to use in blackhole attack?

3. Can we use this model in our real life ?

1.5 Expected Output

Simulation of 50 nodes vehicular ad-hoc network by using ns2 is performed. In TCL file we make some nodes as malicious and see the output by the network protocol that modified to detect the blackhole node by using the predefined variable in the TCL file of the corresponding node. The detecting output shows in the terminal window. The effect of the attack is stored in the trace file. Simulation can be shown in animation using netanim.

1.6 Report Layout

This report is divided into 5 chapters and they are
Chapter 1: Introduction
Chapter 2: Background
Chapter 3: Research Methodology
Chapter 4: Experimental Results and Discussion
Chapter 5: Conclusion and Implication for Future
At the end of the paper, we add References and Appendices
Abstract is placed at the very first of the paper.

Chapter 2

Background

2.1 Introduction

VANET is a kind of MANET with vehicular node. Traffic has a great impact on the economy of the 21st century. For the safer and flawless network on the road, we have to use a better protocol and some applications like IDS, IPS.

2.2 Related Works

H. Deng et al.[2] discussed a protocol that requires intermediate nodes for sending RREP message along with the next-hop information. When the source node gets this information, it sends an RREQ to the next hop to verify that the target node indeed has a route to the intermediate node and the destination. When the next hop receives a Further Request, it sends a Further Reply which includes the check result to the source node. Based on information in Further Reply, the source node judges the validity of the route. In this protocol, the RREP control packet is modified to contain the information about next-hop. After receiving RREP, the source node will again send RREQ to the node specified as next hop in the received RREP.

B. Sun et al. [3] use AODV as their routing protocol and simulation is done in the ns2 simulator. The detection technique is a neighborhood-based method to detect the black hole attack and then present a routing recovery protocol to build the the real path to the destination. Based on the neighbor set information, a method is improved to deal with the black hole attack. Source node sends a modify-Route-Entry (MRE) control packet to the Destination node to form a correct path by modifying the routing entries of the intermediate nodes (IM) from source to destination.

S. Ramaswamy et al. presented an algorithm in [4] which claims to prevent the black hole attacks in ad-hoc network. In this algorithm each node maintains additional data packets, a node must show its honesty. If a node is the first receiver of an RREP packet, it forwards packets to source and initiates the judgment process on about replier. The judgment process depended on the opinion of the network's nodes about replier. These neighbors are requested to send their opinion about a node. When a node collects all opinions of neighbors, it decides if the replier is a malicious node based on number rules.

M.Y. Su [5] proposed the mechanism to detect and separate malicious nodes, which selectively perform black hole attacks by deploying IDSs in MANETs (mobile ad hoc networks). All IDS nodes perform an ABM (Anti-Black hole Mechanism), which estimates the suspicious value of a node, according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. With the prerequisite that intermediate nodes are forbidden to reply to RREQs if an intermediate node, which is not the destination and never broadcasts an RREQ for a specific route, forwards an RREP for the route, then its suspicious value will be increased by 1 in the nearby IDS's SN (suspicious node) table. When the suspicious value of a node exceeds a threshold, a Block message is broadcasted by the detected IDS to all nodes on the network to cooperatively isolate the suspicious node.

Some attempts have been made for securing wireless monile communication, such as: Secure Efficient Ad hoc Distance vector routing protocol (SEAD) [6], the secure on-demand routing protocol - Ariadne [7], authenticated routing for ad hoc networks (ARAN) [8], Security-aware ad hoc routing (SAAR) [9], Resiliency Oriented Secure (ROS) [10], Secure Routing Protocol (SRP) [11], Secure AODV (SAODV) [12], Secure Link- State Protocol (SLSP) [13], Cooperative Security-Enforcement Routing (CSER) [14]

2.3 Research Summary

A solution is proposed to identify a black hole node, remove that node from the routing table and finally added to the blacklist table. The layout of the network is given below.

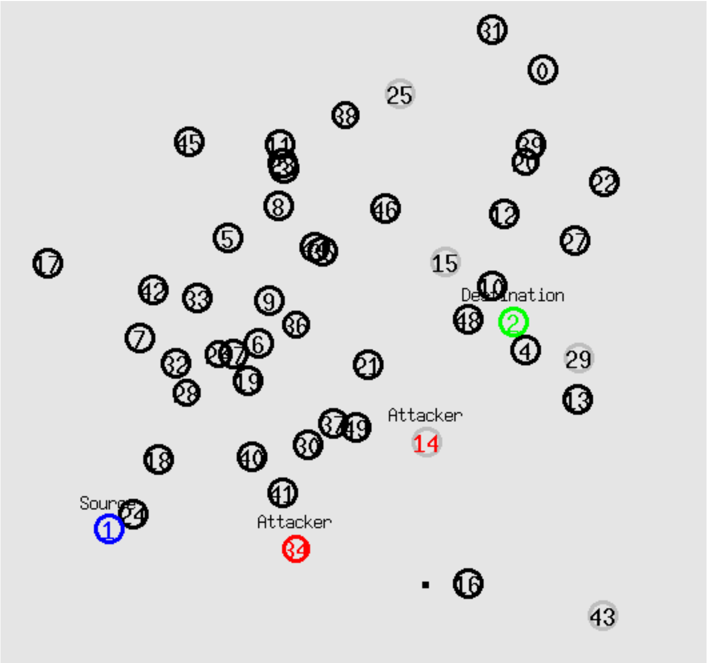


FIGURE 2.1: Layout of Network

2.4 Scope of the Problem

The purpose of the work is to make a secured network where the blackhole attacker is detected and marked as a malicious node. 50 noded network is used in this study and

make 3 of them as malicious. Whenever they drop the packet from a legitimate node. The simulation is run 8 min and Sent total 616 packet
To detect the malicious node we had slightly enhanced the AODV protocol working. In our approach, when the sender broadcasts the RREQ packet, it will wait for reply. If the hop count is very short every time then the node is marked as a malicious node.

2.5 Challenges

Vehicular ad-hoc network is a self-composing network with a highly dynamic network topology. For its dynamicity, though it has many advantages it faces some safety issues. That fall it in threat. If we can fix those issues, VANET can be use heedlessly.
For the Exporting graph from the trace file, there is no much available application. We used a very old software named tracegraph.
Vanet is complex compared to other mobility networks.

Chapter 3

Research Methodology

In this work, the aodv protocol slightly enhanced for making this protocol to detect blackhole node. Have to add some extra code in the header file of the protocol. The routing table and receive request is modified for this system build.

3.1 Introduction

Blackhole node is detected by this system. and information about detection is sent in the terminal. Admin may block this particular node from this network.
AODV protocol depends on some header files. we should have configured those files also.
In this project, the nature of the blackhole attack is used to detect the blackhole node.

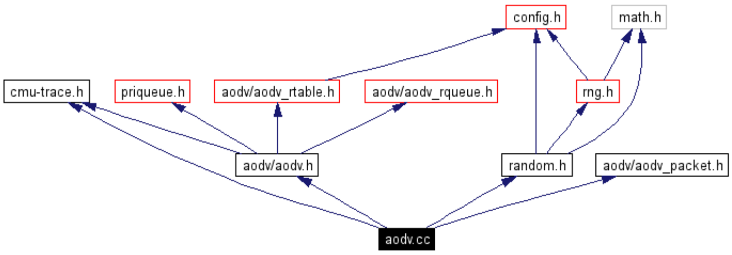


FIGURE 3.1: Dependencies of aodv.cc

The main purpose of this work to detect malicious node in a crowded road where the blackhole mislead us in a wrong road where there is a barricade or the road is blocked.

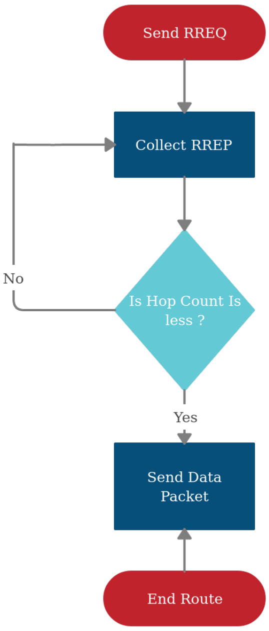


FIGURE 3.2: Work Flow

3.2 Research Subject and Instrumentation

First of all, A VANET is created using OSM. This file is used as a source of the TCL file of the network that takes up from the ns2 package. The TCL file is used to mark a node as malicious. After that, aodv.cc and aodv.h is edited to implement the main detection algorithm.

In Blacklist table, each node will check its table to identify whether the packet is coming from the malicious node. If this is true, it will discard the packet. Also when any node identifies the malicious node, it will send alarm packets to the entire network about the malicious behaviors of the node thereby removing the node from the routing table and adding it in the blacklist table.

3.2.1 SUMO

Sumo is an application to generate a vanet network. we use two tools of sumo application and they are
1. osm web wizerd
2.trace exporter

osmWebWizerd is used to get real-time data from the map and generate a network scenario. After that, we use trace exporter to convert this scenario to a trace file.

3.2.2 NS2

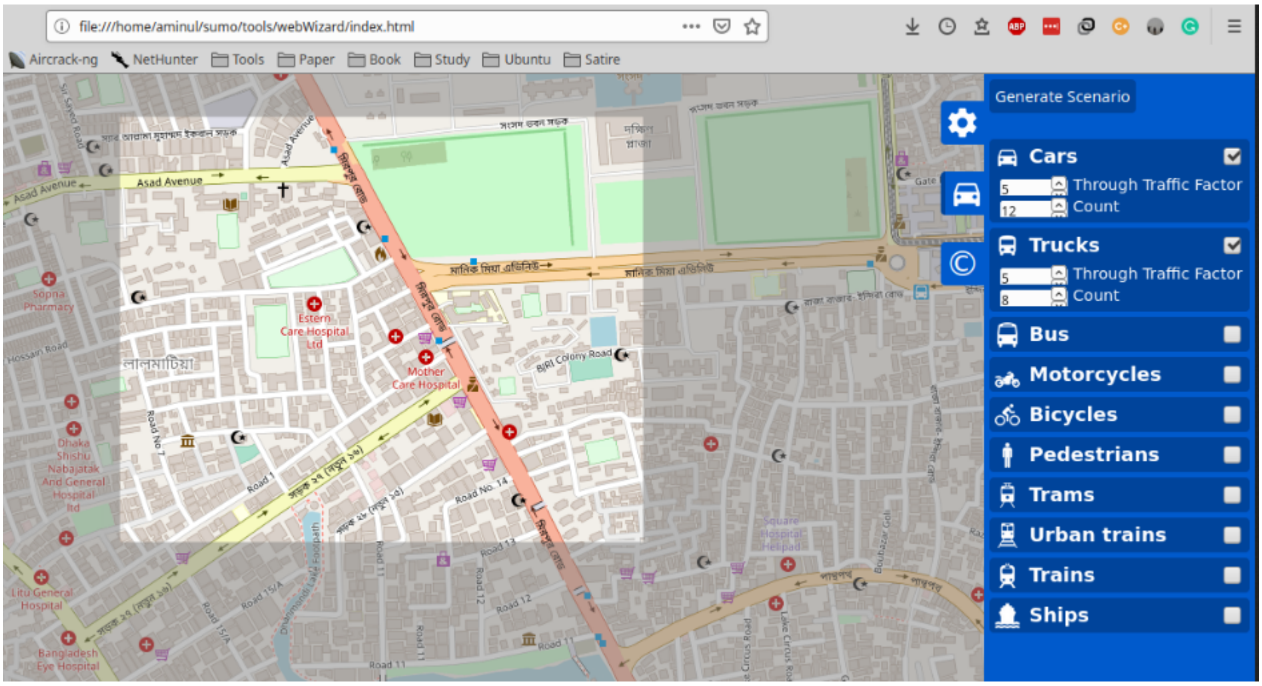
It is a discrete-time simulator. The designed protocol can be applied in it. NS2 is a mostly used open-source simulation application.
Though there is a new version of ns named ns3, the older version is used because of having efficient knowledge in ns2.

3.2.3 Tracegraph

The trace file is analyzed with tracegraph. Two trace file (with malicious node, without malicious node) is created, observing both files and see the difference in between them. Three parameter is used in this project.

3.3 Data Collection Procedure

Auto-generated traffic mobility data is created with sumo application. It auto-generates in real-world locations and has information about authentic data. It uses python package as it's design.



file:///home/aminul/sumo/tools/webWizard/index.html

Generate Scenario

Cars ☑
5 Through Traffic Factor
12 Count

Trucks ☑
5 Through Traffic Factor
8 Count

Bus □

Motorcycles □

Bicycles □

Pedestrians □

Trams □

Urban trains □

Trains □

Ships □

FIGURE 3.3: Data Collection

3.4 Implementation Requirements

Requirements of this project are

1. Basic command of the Linux operating system.

2. Clear idea about network and routing.

3. NS2 is the simulation application. Have to have an idea about build and change routing code of it.

4. analyzation of simulation performed using tracegraph. Basic parameter of a network like throughput, jitter cumulative sum, etc.

5. All ns2 code is written in C++. Have to have the ability to understand those code.

Chapter 4

Experimental Results and Discussion

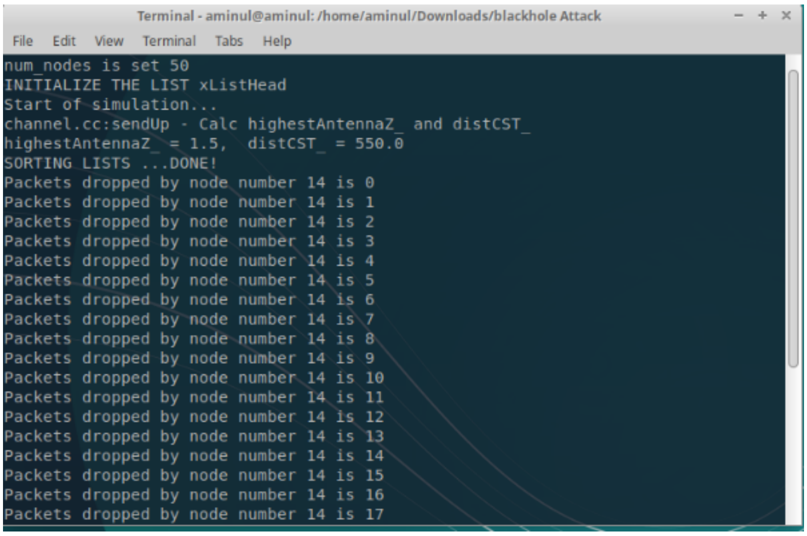
Malicious nodes detected properly by this simulation. When a blackhole node drops a packet the IDS detects the blackhole and gives output in the terminal.[4.1] And send the malicious node to the blacklist.

4.1 Introduction

In this simulation, blackhole node is detected in ns2. AODV is a reactive routing protocol. When the source node searches the route for communication. It sends RREQ to the neighbor nodes and sends the RREP to the route 1st hop. If 1st node drops the packet the message is sent to the admin that which node drop whose packet. A comparison between with and without blackhole is given in the table. 4.1

Parameter	**With Blackhole**	**Without Blackhole**
Simulation time in seconds	7.969744514	7.996721981
Number of nodes	50	50
Number of sent packets	679	1148
Number of dropped packets	693	616
Average packet size	63.6649	83.0259
Number of dropped bytes	82048	66566

Table 4.1: Simulation Comparison Of Blackhole Attack


Terminal - aminul@aminul: /home/aminul/Downloads/blackhole Attack
File
Edit
View
Terminal
Tabs
Help

```
num_nodes is set 50
INITIALIZE THE LIST xListHead
Start of simulation...
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
Packets dropped by node number 14 is 0
Packets dropped by node number 14 is 1
Packets dropped by node number 14 is 2
Packets dropped by node number 14 is 3
Packets dropped by node number 14 is 4
Packets dropped by node number 14 is 5
Packets dropped by node number 14 is 6
Packets dropped by node number 14 is 7
Packets dropped by node number 14 is 8
Packets dropped by node number 14 is 9
Packets dropped by node number 14 is 10
Packets dropped by node number 14 is 11
Packets dropped by node number 14 is 12
Packets dropped by node number 14 is 13
Packets dropped by node number 14 is 14
Packets dropped by node number 14 is 15
Packets dropped by node number 14 is 16
Packets dropped by node number 14 is 17
```

FIGURE 4.1: Output in terminal

4.2 Experimental Results

In this simulation 50 nodes is used and this simulation took place for around 8 min. Both with and without blackhole nodes the simulation performed and observed the output. It is observed that when the blackhole nodes are presented packet was sent in huge in number and drop rate is also higher. Throughput of generated packets are decreases almost 50% less with 3 blackhole nodes among 50 nodes.

Three parameters are considered in this simulation. They are:
1.Cumulative Sum
2.Throughput
3.Jitter

4.2.1 Cumulative Sum

It is a sequential analysis process. It is used to monitoring change detection. In a network, cumulative sum indicates the use of the network. when the malicious node is present the traffic of the network increases so the cumulative sum increased. [15]

Parameter	**Nature**	**With Blackhole**	**Without Blackhole**
generated packets	Minimum	1.00	1.00
	Average	374.50	583.50
	Maximum	748.00	1166.00
sent packets	Minimum	1.00	1.00
	Average	315.00	560.50
	Maximum	629.00	1120.00
forwarded packets	Minimum	1.00	1.00
	Average	19.50	71.50
	Maximum	38.00	142.00
received packets	Minimum	1.00	1.00
	Average	630.00	522.50
	Maximum	1259.00	1044.00
dropped packets	Minimum	1.00	1.00
	Average	347.00	308.50
	Maximum	693.00	616.00

TABLE 4.2: Cumulative Sum Of Dropped Packets Simulation

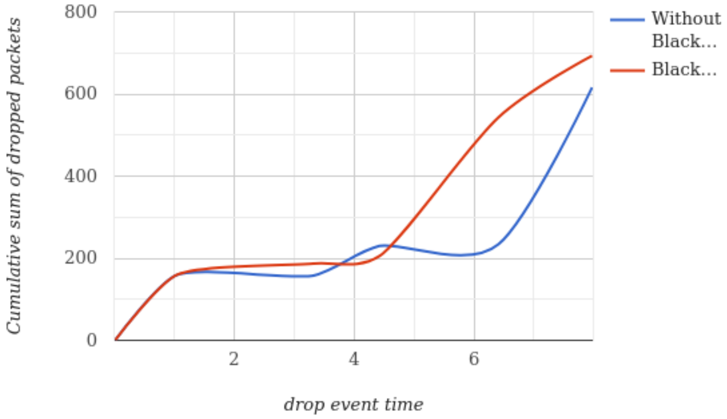


FIGURE 4.2: Cumulative sum of dropped packets

Parameter	Nature	With Blackhole	Without Blackhole
generated packets	Minimum	1.00	1.00
	Average	83.11	129.55
	Maximum	220.00	220.00
sent packets	Minimum	1.00	1.00
	Average	69.89	124.44
	Maximum	165.00	198.00
forwarded packets	Minimum	0.00	1.00
	Average	4.22	15.78
	Maximum	17.00	20.00
received packets	Minimum	1.00	1.00
	Average	139.89	116.00
	Maximum	256.00	231.00
dropped packets	Minimum	1.00	0.00
	Average	77.00	68.44
	Maximum	204.00	213.00

TABLE 4.3: Throughput Of Dropping Packets Simulation

4.2.2 Throughput

It is a transmission measurement parameter. It is a ratio of transmitted traffic and unit of time. It is the best way of measuring a network. If the throughput is higher the traffic of the network is more. We should avoid a system with high traffic.

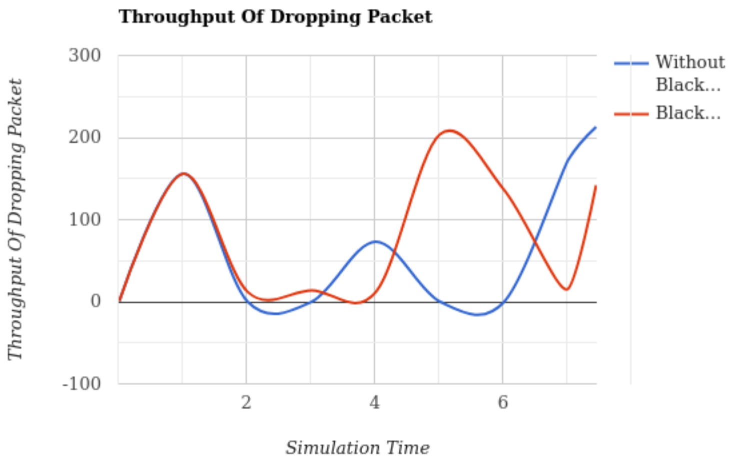


FIGURE 4.3: Throughput Of Dropping Packet

Parameter	Nature	With Blackhole	Without Blackhole
generated packets	Minimum	-0.01	-0.01
	Average	0.11	0.045
	Maximum	0.29	0.28
sent packets	Minimum	-0.01	-0.01
	Average	0.11	0.04
	Maximum	0.29	0.28
forwarded packets	Minimum	-0.01	-0.01
	Average	0.11	0.05
	Maximum	0.28	0.28
received packets	Minimum	0.01	0.01
	Average	0.15	0.20
	Maximum	0.37	0.37
dropped packets	Minimum	0.00	0.00
	Average	0.10	0.14
	Maximum	0.40	0.38

TABLE 4.4: Jitter Of Dropped Packets Simulation

4.2.3 Jitter

It is the variance in the time delay between a data packet over a network. It is defined as to disturb in normal packet sending sequence. Jitter helps in decision making about a network.

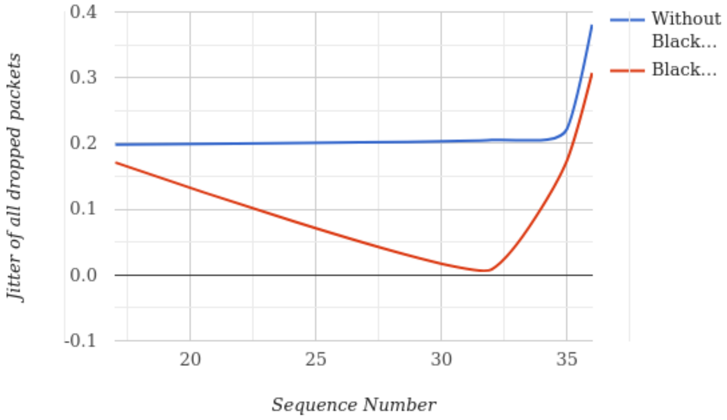


FIGURE 4.4: Jitter of dropped packets

4.3 Descriptive Analysis

50 nodes simulation when 3 of them are blackhole is observed. In this process of identification every node is observed. The network size doesn't matter in this case. Ad-hoc on demand routing is most used and efficient routing protocol. It is secured in nature. Result of this project is satisfectory.

4.4 Summary

It observed that the cumulative sum of packet dropping increases 12.66% for 3 malicious nodes.
At same way throughput of dropping packet increase by 12.51 % & average jitter of dropping a packet is increased by 40%.

Chapter 5

Conclusion and Implication for Future

5.1 Summary of the Study

This simulation is based on blackhole attack detection in a vanet when aodv is using as a routing protocol. Vanet is used in the vehicle so it has a huge impact in real life. And many network-level attackers prefer blackhole attack because it maintains communication between legitimate nodes and drops packet.

5.2 Conclusions

Despite a large number of vehicles in this simulation, this process of detection blackhole is proper and the process that we use is so far won't used yet. The parameters of the simulation give a clear idea about the blackhole. Considering three parameters helps to decide the accuracy of this work.

5.3 Recommendations

Vanet is a new technology in traffic maintenance and driving support system. Much work is done in the field of vanet nowadays. they are maximum on the security issue. Mainly in the aodv protocol.

P. Anand Babu designed attack detection in vanet. Information about the attacker is stored in the knowledge base.

5.4 Implication for Further Study

Though blackhole detection is efficient it can't detect any malicious node with its previous knowledge. No machine learning is used here. Using machine learning make this an uncomputable detection tool.

Simulation has occurred 8 minutes and 50 nodes. If this simulation is run for more time with a more nodes the result will be more accurate and proper.

In this work, simulation is tested only in aodv protocol. In the future, another protocol may be implemented.

References

[1] The new york times, 2016. the bangladeshi traffic jam that never ends.

[2] Hongmei deng, wei li and d. p. agrawal, "routing security in wireless ad hoc networks," in ieee communications magazine, vol. 40, no. 10, pp. 70-75, oct. 2002.

[3] Bo Sun, Yong Guan, Jian Chen, and Udo W Pooch. Detecting black-hole attack in mobile ad hoc networks. 2003.

[4] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall E Nygard. Prevention of cooperative black hole attack in wireless ad hoc networks. In *International conference on wireless networks*, volume 2003, pages 570–575, 2003.

[5] Ming-Yang Su. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *Computer Communications*, 34(1):107–117, 2011.

[6] Yih-Chun Hu, David B Johnson, and Adrian Perrig. Secure efficient ad hoc distance vector routing. In *the Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and applications (WMCSA'02)*, 2002.

[7] Yih-Chun Hu, Adrian Perrig, and David B Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. *Wireless networks*, 11(1-2):21–38, 2005.

[8] Kimaya Sanzgiri, Daniel LaFlamme, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth M Belding-Royer. Authenticated routing for ad hoc networks. *IEEE Journal on selected areas in communications*, 23(3):598–610, 2005.

[9] Aagrah Sharma, Dhruv Zaveri, Gitanshu Yadav, and Suyog Pande. Security and qos aware dynamic clustering (sqadc) routing protocol for crn: A review. 2018.

[10] J Martin Leo Manickam and S Shanmugavel. Providing routing security using ros protocol in manet and performance comparison with aodv. *Information Technology Journal*, 6(5):656–663, 2007.

[11] John Marshall, Vikram Thakur, and Alec Yasinsac. Identifying flaws in the secure routing protocol. In *Conference Proceedings of the 2003 IEEE International Performance, Computing, and Communications Conference, 2003.*, pages 167–174. IEEE, 2003.

[12] Mohaned Juwad and Hamed S Al-Raweshidy. Experimental performance comparisons between saodv & aodv. In *2008 Second Asia International Conference on Modelling & Simulation (AMS)*, pages 247–252. IEEE, 2008.

[13] Panagiotis Papadimitratos and Zygmunt J Haas. Secure link state routing for mobile ad hoc networks. In *2003 Symposium on Applications and the Internet Workshops, 2003. Proceedings.*, pages 379–383. IEEE, 2003.

[14] Bin Lu and Udo W Pooch. Cooperative security-enforcement routing in mobile ad hoc networks. In *4th International Workshop on Mobile and Wireless Communications Network*, pages 157–161. IEEE, 2002.

[15] Haoyu Gao, Mingyao Luo, Kun Fang, Bowen Fan, Jiawei Zhao, Yunfei Xue, and Chang Shu. Cumulative sum analysis of the learning curve for the preclosure technique using proglide. *Interactive CardioVascular and Thoracic Surgery*, 30(2):280–286, 2020.

Appendices

.1 Research Reflection

This work helps to detect blackhole node in vanet.This norm can be used to get a safe and trust worthy road. Populated country like bangladesh it helps to metigate road accident and traffic jam which has a great impact in economy.

.2 Related Issues

In this project we work for detection of blackhole attack in vanet. We can't design any system to prevent blackhole node automatically. Though we can manually block the blackhole node.
There are some other attack in vanet like
1.wormhole attack
2.Greyhole attack
3.Byzantine attack
4.Flooding attack