Title

Mitigation and Performance Analysis of Routing Protocols under Hostile Environments in Vehicle Ad-Hoc Networks (VANETs)

Author information

Adam Gorine and Ayoade Adeyemo

Institute: University of the West of England, Department of Computer Science and Creative Technologies, Bristol, United Kingdom.

Email: adam.gorine@uwe.ac.uk

ORCID: **0000-0001-7378-8933**

Abstract

This research will compare two main VANET protocols, Dynamic Source Routing (DSR) and Ad-Hoc On-Demand Distance Vector (AODV), subjected to two malicious attacks: blackhole and wormhole attacks. Then propose a mitigation method to countermeasure these attacks.

This research uses NS3 to simulate a network of 100 nodes spread across a terrain of 300x1500 m^2 with a simulation time of 10 seconds.

The simulation aims to measure the Average Throughput (ATP), End-to-End average delay (AEED), Packet Delivery Ratio (PDR) and Packet Loss Ratio (PLR) from the data gathered during the simulations to evaluate the performance of the network.

The results generated from this investigation show that DSR performs better than AODV regarding the average end-to-end delay, Packet Delivery ratio and packet loss balance when subjecting these two protocols to blackhole and wormhole attacks. However, AODV outperforms DSR when measuring the average throughput under the same attacks.

To countermeasure the effect of the malicious node on the VANET protocol, a proposed algorithm called soft encryption is applied to mitigate these attacks. The proposed algorithm aims to detect misbehaving nodes, isolating them from the network and dropping their packets. On the other hand, reward the well-behaving nodes by forwarding their traffic.

Keywords

AODV protocol, DSR protocol, VANET, Blackhole Attack, Wormhole Attack, NS3.

1. INTRODUCTION

The ultimate goal of Connected and Autonomous Vehicles (CAV) is to promote traffic management, improve road safety, enhance people's travelling experiences, reduce road traffic accidents, and eventually save lives. Car manufacturers invest heavily in research and development to equip vehicles with various wireless communication devices, GPS and advanced A.I. algorithms that allow them to share information between vehicles and roadside infrastructure. As a result, these vehicles will operate without a driver's assistance. They can navigate in densely populated cities and detect traffic congestion and road incidents, enabling them to choose the shortest and most efficient route to their destination with the minimum time and fuel cost [1].

2. VEHICLE AD-HOC NETWORKS (VANETs)

2.1 VANET Technology

VANET is a self-organising ad-hoc network in which vehicles represent nodes [2], as shown in Figure 1. Nodes are dynamic as cars move at high speed and change their position frequently within limited road topology. Each vehicle or node contains the following components [3]:

- On-Board Unit (OBU): OBU exchanges messages with Roadside Units and other OBUs. VANET shares many characteristics of Mobile Ad Hoc Networks (MANETs) with added services such as inter-vehicular communication (IVC), which allows cars, roadside units, and adjacent pedestrians to share information within a predetermined range [4].
- Application Unit: It is embedded in a vehicle or a general device such as a personal digital assistant. The application unit can only communicate with the roadside unit using a wireless channel.
- Roadside Unit: This unit is installed along both sides of the road, road intersections or parking spaces. It can also be used as an early warning of traffic incidents and to connect to the Internet.

- Sensors: Usually includes an ultrasonic sensor, radar, LiDAR, Global Position Systems (GPS)

2.2 VANETs Communications:

VANET supports three types of communications [5] which are described and shown in Fig.1 below:

- Vehicle-to-Vehicle (V2V): one vehicle communicates with other vehicles within communication range. V2V communication is achieved using dedicated short-range communication (DSRC) or Wi-Fi.
- Vehicle-to-Infrastructure (V2I): The communication between vehicles and roadside units (RSU). V2I uses dedicated short-range communication (DSRC), like the technology used for vehicle-to-vehicle communication.
- Vehicle-to-Everything (V2X) refers to the communication between vehicles and any internet-enabled device.

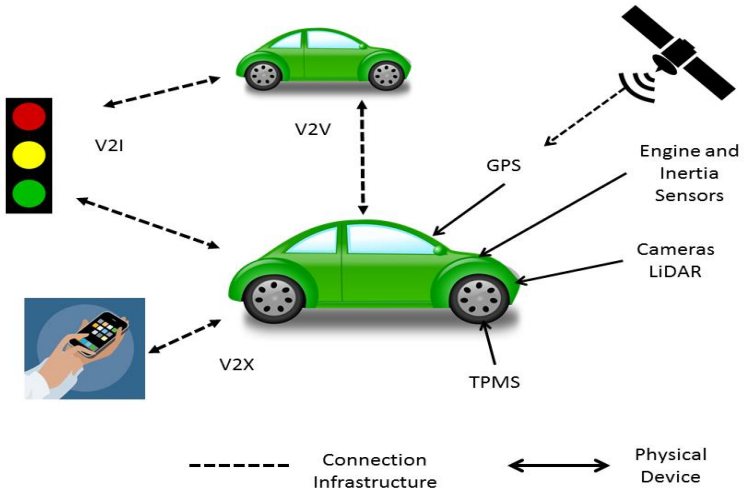

Fig.1 Vehicle Ad-Hoc Networks Structure [1]

3. VANETs PROTOCOLS

There are many standard VANET routing protocols which include: Ad hoc on-demand vector (AODV), dynamic source routing (DSR), Dynamic MANET on-demand (DYMO), optimised link state routing protocol (OLSR), Greedy perimeter stateless routing (GPSR), Geographic source routing (GSR), Geographic routing protocol (GRP) [6]. This paper will focus on AODV and DSR protocols. But first, I will briefly explain these two protocols and their operation.

3.1 Ad-Hoc On-Demand Vector (AODV) Protocol:

AODV is a routing protocol used in wireless and vehicle ad-hoc networks. It only establishes a route between two cars when the source vehicle requires it (i.e. on demand).

3.2 Dynamic Source Routing (DSR) Protocol:

DSR is a self-maintaining and efficient routing protocol for Mobile Ad-hoc Networks and requires each source node to maintain a route to destination pairs. It operates using two components; Route Discovery and Route Maintenance.

4. CYBER ATTACKS ON VANETs

VANETs are more vulnerable to attacks due to a lack of infrastructure and the dynamic nature of the network, which can sometimes damage the confidentiality, Integrity, and availability of connections between Vehicles [6]. In this research paper, we investigated two malicious attacks: wormhole and black hole attacks. A short description of both attacks is given below:

4.1 **Wormhole attacks**

In this attack, two malicious nodes form a virtual tunnel sending data from one end of the tunnel to the other [7]. When packets are tunnelled to a completely different network location, both AODV and DSR protocols reveal that route discovery will include a path through the wormhole. Once this malicious node has gained confidence, all traffic destined for this node will be dropped, resulting in network performance degradation**.**

As shown in Fig.2, the malicious node (M1) receives RREQ from the source (S) and tunnels it to another malicious node (M2) before forwarding it to the destination node (D) in a reactive routing environment. Node (D) sends RREP on the (D-M2-M1-S) route since it is the first to reach it. As a result, the malicious nodes form a tunnel and direct traffic through it.

Fig.3 gives definitions of all the abbreviated components involved in a wormhole attack.

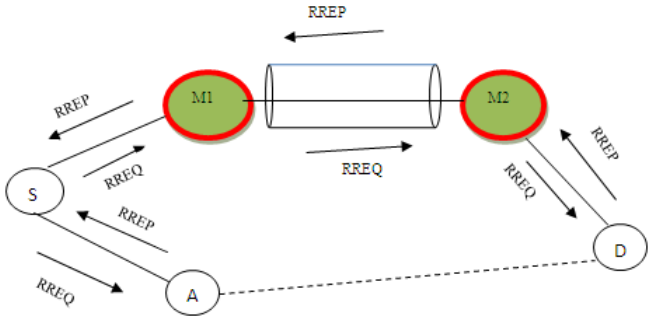

Fig.2 Structure of wormhole attack [8]

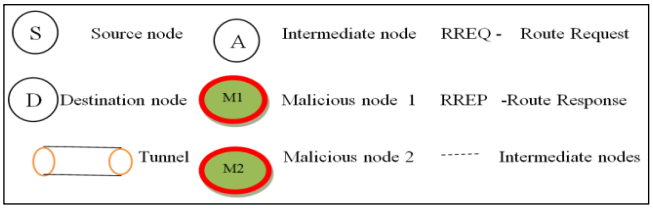

Fig.3 Wormhole attack parameters [8]

4.2 **Black Hole Attacks*:***

During a blackhole attack, the source node sends a route request (RREQ) to the destination in a reactive routing environment, in which the intermediate nodes provide RREP in response to the RREQ. At the same time, the malicious node will send an RREP in response, claiming that it has found the shortest path to the target node. From that point onward, the source node will route all packets via the malicious node, thinking it is the shortest path to the destination. The malicious node will drop all packets, causing a decreased packet delivery ratio.

Fig.4 shows how a Node (S) uses RREQ to find a route to Node (D). The malicious node (M) tricks node (S) by responding with RREP, claiming it has the shortest path to the destination (D). Therefore, node (S) unintentionally transmits the packet to node (M), which drops the packet causing a denial of service.

Fig.5 gives definitions of all the abbreviated components involved in a blackhole attack.

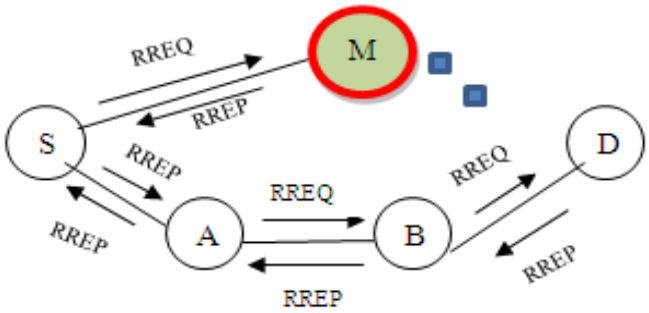

Fig.4 Blackhole attack structure [8]

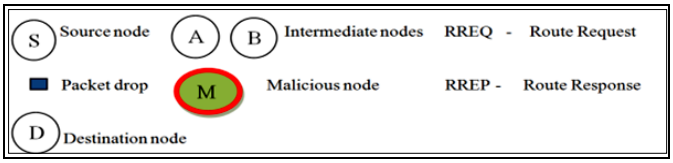

Fig.5 Blackhole attack parameters [8]

5. RELATED WORK

This section describes and critically analyses previous work on cyber-attacks on VANETs. In the beginning, VANETs security was not a big priority when developing VANETs protocol which caused many security issues later.

The authors of the paper [9] investigated the performance of two protocols, OLSR and AODV, in urban road scenarios based on two roads and multiple junctions. The performance is measured using four parameters: PDR, overhead, throughput, and End-to-End delay. In two density variation situations with transmission ranging from 250 and 500m, the authors employed CBR for data traffic. According to the authors, both systems' routing costs and delays doubled with density. Their results stated that AODV and OLSR protocols were ineffective in a VANET with a high vehicle density.

In one study in [10], the authors investigated the effect of blackhole attack on VANETs Ad-Hoc On-Demand Distance Vector (AODV) protocol by measuring the Packet Drop Rate, Throughput and End to End Delay Parameters. They used NS2 as a network simulation for 100 vehicles. They found the packet Drop Rate, Average End to End Delay to be high and throughput to be low under blackhole attacks.

In conclusion, AODV has some limitations and is the most vulnerable protocol when subjected to blackhole attacks.

In [11], researchers used an NS-2 simulator with 50 nodes, injection of six malicious nodes within the network, and a packet size of 512 bytes. The simulation area is 1000 X 1000 m at a speed of 10m/sec with a total simulation time of 250 seconds. Their result shows malicious nodes negatively influence AODV network performance regarding throughput, packet delivery ratio, and end-to-end delay.

Researchers in [12] investigated the effect of blackhole and wormhole attacks on AODV protocol. Using NS3 as the network simulation, they measured average throughput, average packet delivery ratio, average end-to-end delay, and average jitter delay.

The results show that Average Throughput in Normal, Blackhole, and Wormhole AODV decreases as the number of nodes increases.

The Average PDR in Wormhole AODV is more significant than in Blackhole AODV because packets drop in a blackhole attack and remain 100% in normal AODV.

In addition, the average end-to-end delay and Average Jitter-Sum delay in Wormhole attacks are more significant than in normal operations and during blackhole attacks.

In conclusion, overall, Wormhole Attack is more dangerous for the network performance than normal and Blackhole Attacks.

The authors in [14,15] investigated the impacts of black holes, flooding, and hasty attacks on AODV. First, they evaluated the performance of the AODV under attack to the original AODV in terms of the packet loss ratio, packet delivery ratio, average end-to-end delay, and average throughput. They concluded that AODV's performance deteriorates during attacks. Furthermore,

they said Black hole attacks significantly impacted network performance more than flooding and rushing attacks.

Recently researchers [18] developed a novel methodology using the Eclipse MOSAIC simulation framework to model two typical road traffic scenarios capturing communication between vehicle to vehicle (V2V) and vehicles to infrastructure (V2I) in which attacks are introduced in the form of replay and bogus messages. The model generated an open dataset for developing machine learning algorithms for anomaly detection and mitigation solutions to enhance security in VANET communications.

6. METHODOLOGY

Simulation is a critical methodology to experiment with VANET protocols rather than using actual vehicles. The simulation of VANETs is divided into two components:

6.1 Traffic Simulation:

Generate position and movement information of a single vehicle in VANETs environment. For example, the Institute of Transportation Systems developed SUMO (simulator for urban mobility) at the German Aerospace Centre [13]. SUMO models individual vehicles and their interactions using models for ca-following, lane-changing and intersection behaviour.

6.2 Network Simulation:

Various open-source VANETs simulators are available, including NS2, NS3, NCTUns, GlomoSim and OMNET++; selecting convenient tools for measuring network performance is frequently tricky without a complete analysis of existing tools.
NS3 is the simulator of choice in this research as it is the latest network simulator for education and research.
NS3 simulator is a discreet-event network simulator for Internet Systems based on a library written in C++ as described in [16].
The network consists of 100 nodes spread across a terrain of 300x1500 m^2 with a simulation time of 10 seconds. The simulation aims to measure a few parameters, including the *average throughput* (ATP), average *end-to-end delay* (AEED), *packet delivery ratio* (PDR), and *packet loss ratio* (PLR) from the data gathered during the simulations to evaluate the performance of the network.

The parameters used to measure the network performance are described below:

***Packet Delivery Ratio (PDR)*:**

This measurement shows the ratio between the number of packets originated by the source and the number of packets successfully received by the sinks at their target destinations. The PDR shows how a protocol successfully delivers packets from source to destination. The higher the PDR ratio, the better the network performance is. It characterises both the completeness and correctness of the routing protocol. This metric is calculated by dividing the number of packets received by destinations over the number of packets originated from sources as shown below :

$$PDR = (\text{Packets Received} / \text{Packets Sent}) \times 100$$

***Packet Loss or Dropped*:**

Measures the number of transmitted packets that did not reach their destination. Transmitted packets may be lost when a packet reaches the misbehaving nodes that are designed to drop the packets.

This metric measures data lost by the protocol and includes the data that the source or intermediate nodes drop during the simulation time. It can be calculated using the formula below:

$$\text{Packet Dropped \%} = (\text{Packets Sent} - \text{Packets Received}) / \text{Packets Sent}$$

Average End-to-End Delay (AEED): The average time data packets take to travel from the source to the destination node under normal conditions or attacks.

$$AEED = (\text{total time for a packet received} - \text{total time for a packet sent}) / \text{number of received packets}$$

Average Throughput (ATP): is the total number of packets received successfully by the destination node when the network is in normal or under attack conditions.

$$ATP = 100 \times (\text{Packets Received} / \text{Simulation Time})$$

This research investigates security issues in VANETs protocols and focuses on analysing the vulnerabilities of two protocols, AODV and DSR, by subjecting them to Blackhole and wormhole attacks.

To countermeasure the malicious node's effect on the VANET protocol, a proposed soft encryption algorithm is applied to mitigate these attacks. The proposed algorithm aims to detect misbehaving nodes, isolating them from the network and dropping their packets. On the other hand, reward the well-behaving nodes by forwarding their traffic.

7. SYSTEM DESIGN FOR MALICIOUS ATTACKS

7.1. Algorithm for Blackhole attack in AODV protocol

The algorithm and the flowchart for implementing the blackhole attack in AODV and DSR protocols are shown in Figures 17(a) and 17(b), respectively.

Step 1: Start.
Step 2: Add one or more malicious Vehicles to the network.
Step 3: The source node sends RREQ to its neighbour vehicle.
Step 4: Check if the current node is malicious or not.
Step 5: if the condition is TRUE:
- 5.1 Increase the sequence number with a large number and set the hop count to 1.
- 5.2 The malicious node sends RREP to the source vehicle.
- 5.3 Establish a route path between the originating node and the malicious vehicle.
- 5.4 Send the data packets from the originating node to the malicious vehicle.
- 5.5 The malicious node drops the packet.

Step 6: if the condition is FALSE:
- AODV routing protocol will run normally.

Fig. 17(a): Algorithm for implementing blackhole attack on AODV and DSR protocols.

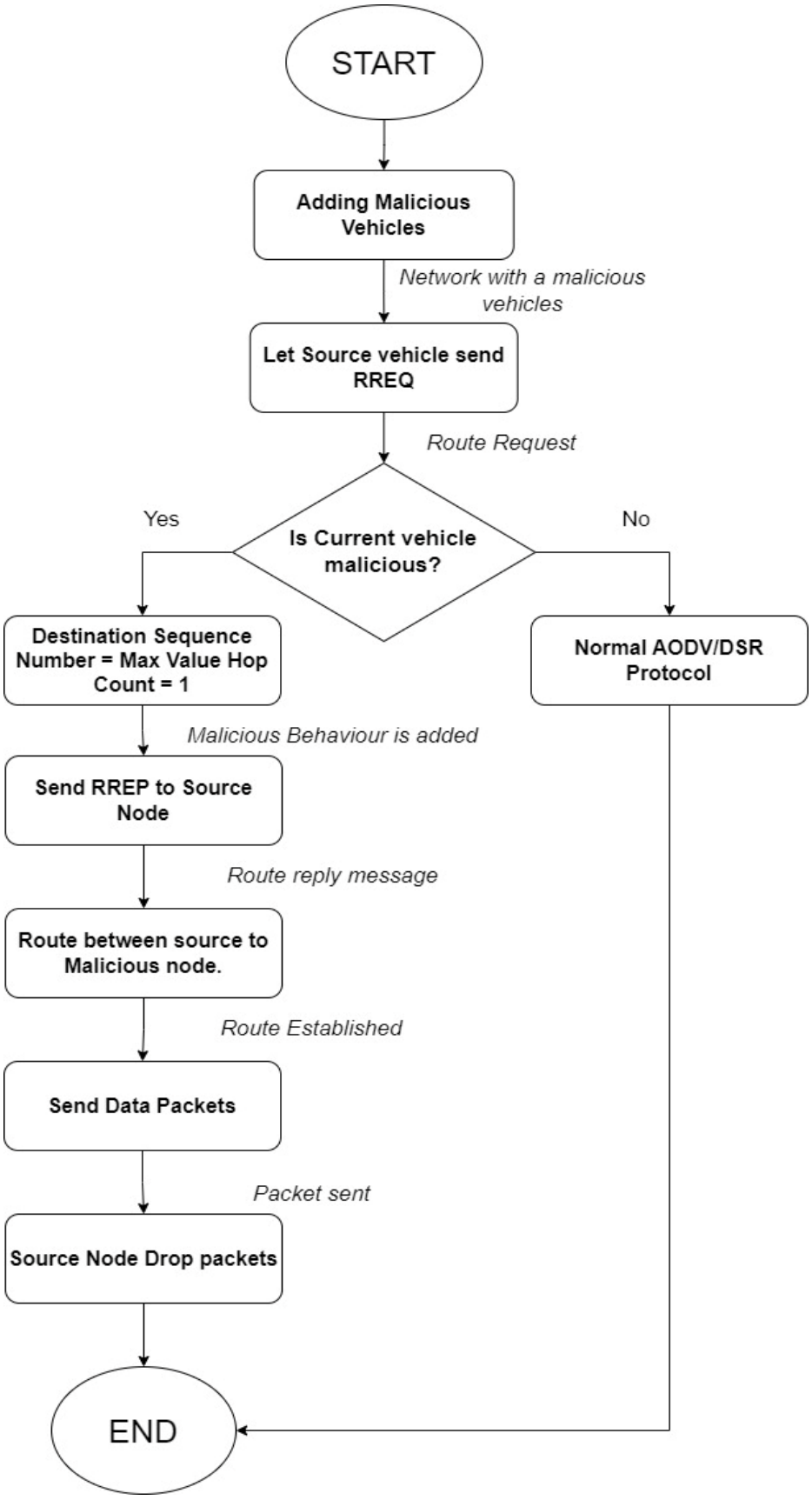

Fig. 17(b): Flowchart for implementing blackhole attack on AODV and DSR protocols

7.2. Algorithm for Wormhole attack in AODV protocol

The algorithm and flowchart for implementing wormhole attacks in AODV protocol are described in 18(a) and 18(b), respectively.

Step 1: Start.
Step 2: Add a malicious node in the network.
Step 3: Divide the malicious vehicle into parts.
Step 4: Set the first part as firstWormHoleTunnel and the second as secondWormHoleTunnel.
Step 4: Allow the source node to send RREQ to its neighbour vehicles.
Step 5: Check if enableWormholeAttack is TRUE and Vehicle is a firstWormHoleTunnel.
Step 6: if the condition is **TRUE**:
- 6.1 Initialise up the count to 1.
- 6.2 Set secondWormHoleTunnel as a receiving vehicle and form a fast tunnel.
- 6.3 secondWormHoleTunnel sends RREQ to its neighbour vehicles.
- 6.4 Let the destination vehicle send RREP messages to the source using a predefined path.
- 6.5 Let the source node vehicle packets to the destination node using a predefined path.
- 6.6 When packets arrive at the firstWormholeTunnel, it should send it to the secondWormHoleTunnel, and it creates a loop.
- 6.7 Drop the packet.

Step 7: if the condition is **FALSE**
Step 8: Check if enableWormholeAttack is TRUE and Vehicle is secondWormHoleTunnel.
Step 9: if the condition in step is true,
- 9.1 Initialise up the count to 1.
- 9.2 Set firstWormHoleTunnel as receiving node and form a fast tunnel.
- 9.3 Let firstWormHoleTunnel send RREQ to its neighbouring nodes.
- 9.4 Let the destination send RREP messages to the source vehicle using a predefined path.
- 9.5 Let source node packets send packets to the destination node using a predefined path.
- 9.6 When packets reach the secondWormHoleTunnel, let it send the packet to the first wormhole tunnel created "firstWormHoleTunnel" and repeat the process.
- 9.7 Drop the packet.

Step 10: if the condition is false:
- 10.1 AODV routing protocol run normally.

Step 11: end.

Fig. 18(a): Algorithm for implementing wormhole attack on AODV and DSR protocols.

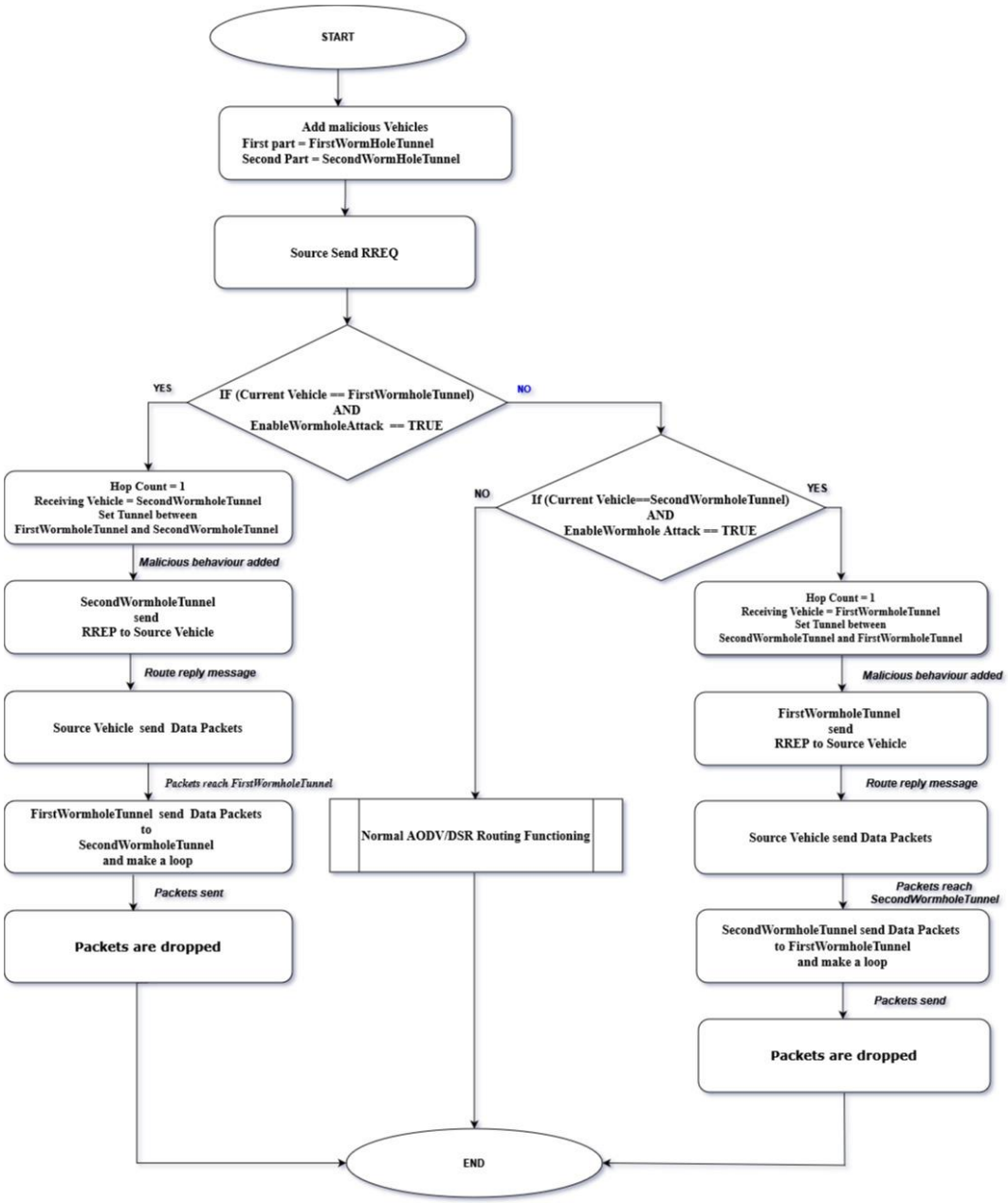

Fig. 18(b): Flowchart for implementing wormhole attack on AODV and DSR protocols.

8. SIMULATION OF ATTACKS AND RESULTS

In this experiment, the performance of two protocols, AODV and DSR, are evaluated in two separate scenarios. The first scenario measures the AODV protocol's performance when we inject the network with percentages of hostile vehicles (i.e. black hole and wormhole attacks) of 15%, 30%, 45% and 60%. The second scenario measures the DSR protocol's performance when the network operates with percentages of hostile vehicles (i.e. blackhole and wormhole attacks) of 15%, 30%, 45%, and 60%, respectively.

The simulation is repeated five times, having the same parameters to get accurate results. Table.1 summarises the parameters used in this experiment.

Simulation Tool	NS-3 (Version 3.28 for normal)
Routing Protocols	AODV and DSR
Packet Size	64[Byte]
Network Area	300 X 1500 m
No of Vehicles	100
% Of Malicious Node	15%, 30%, 45%, 60%
Vehicle Speed	10 m/s
Simulation Time	10 seconds
Performance Metrics	Average Throughput, PDR, AEED, PLR
MAC Protocol	IEEE 802.11p
Data Rates	2.048 kbps/s

Table.1 Summary of the parameters used in the experiment

The simulation results are presented as a series of pairs of graphs (bar charts and line charts). Each pair of graphs shows a comparison of performance between AODV and DSR under malicious attacks. The graphs are organised according to the measured parameter (*packet loss*, *packet delivery ratio*, *average throughput*, average *end-to-end delay*) and the type of attack (blackhole, wormhole):

8.1 Packet loss under blackhole attacks

Fig.6 depicts the packet loss ratio for both protocols when injecting blockholes vehicles, which increases as the percentage of malicious nodes increases. Again, DSR performs better with reduced PLR compared to the AODV protocol.

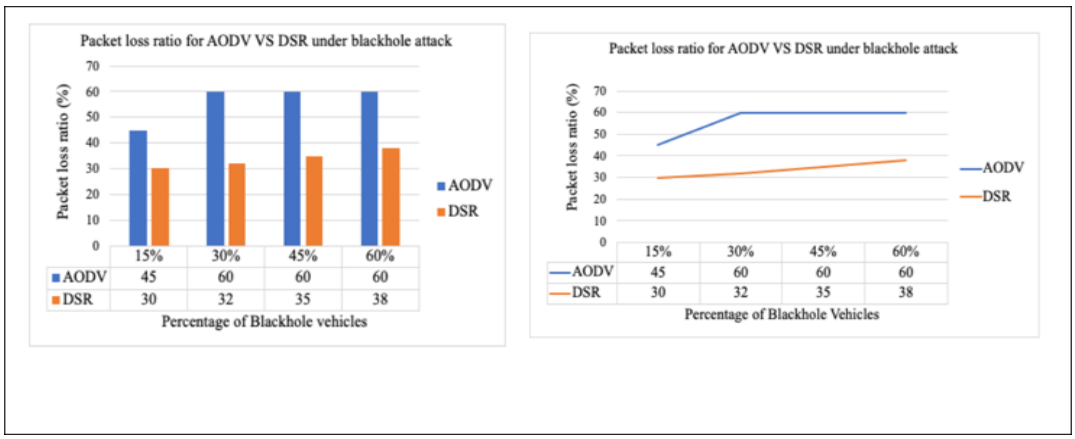

Fig.6 The packet loss ratio for AODV vs DSR under blackhole Attacks

8.2 Packet Delivery Ratio under blackhole attacks

Fig.7 below shows the packet delivery ratio for both protocols, which decreases with increased blackhole attacks within the network. Overall, the DSR protocol still outperforms AODV.

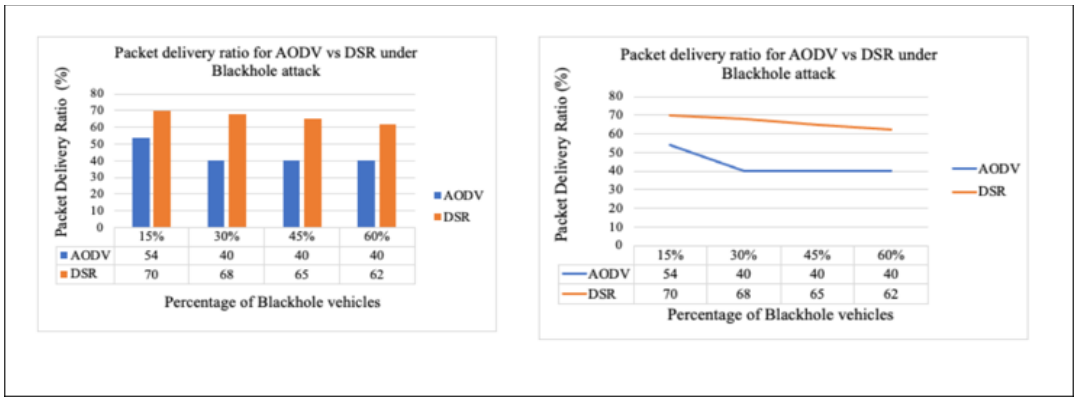

Fig.7 The packet delivery ratio for AODV vs DSR under blackhole Attacks

8.3 Average Throughput under blackhole attacks

Fig.8 describes throughput for both protocols under different percentages of blackhole vehicles. The simulation results show that both protocols are affected by the increase in the ratio of the blackhole vehicle. However, AODV performs better than DSR when the percentage of malicious cars increases.

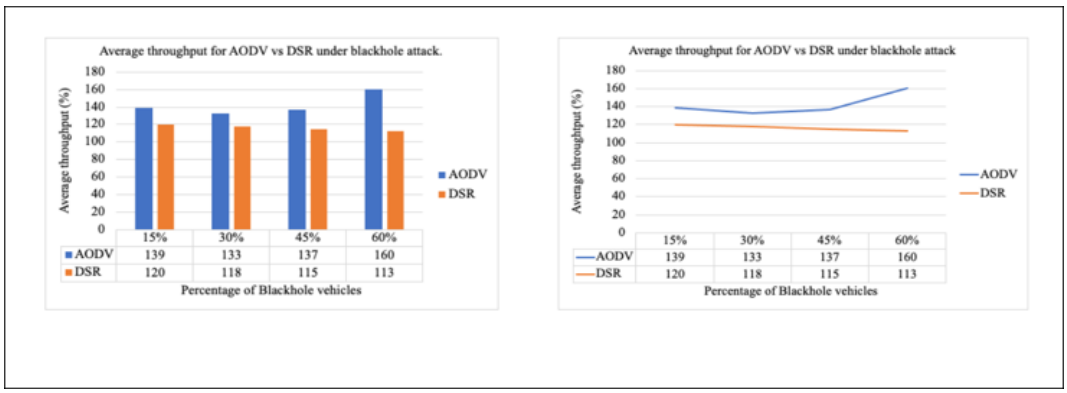

Fig.8 Average Throughput for AODV vs DSR under blackhole attack

8.4 Average End-To-End Delay under blackhole attacks

In **Fig.9** it is observed the average end-to-end delay of both protocols under blackhole vehicles. The two protocols have performed similarly when assessing the average delay metric. The average delay fluctuates with increased blackhole vehicles because the collision is reduced due to the number of dropped packets. Regardless, AODV performed less when compared to DSR.

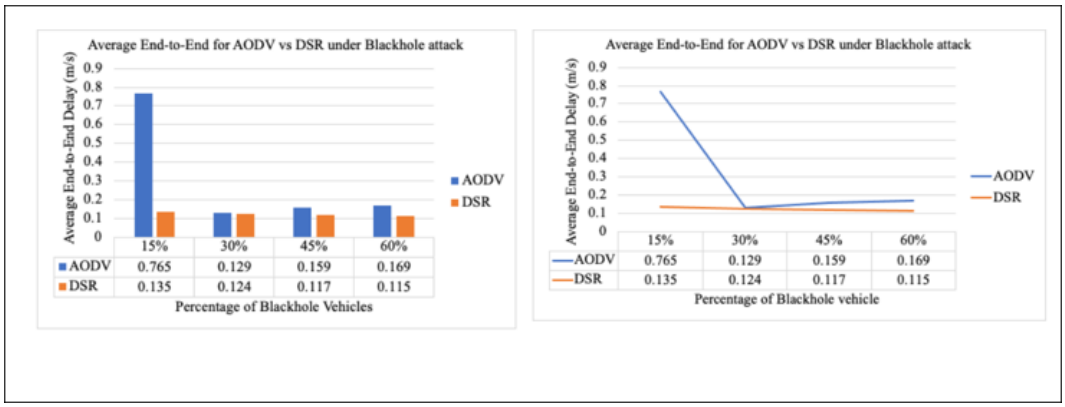

Fig.9 Average End-to-End delay for AODV vs DSR under blackhole attack

8.5 Packet loss under wormhole attacks

The packet loss ratio for both protocols under wormhole vehicles grows as the percentage of the attack increases, as shown in Fig.10. Overall, DSR outperforms the AODV protocol under normal conditions.

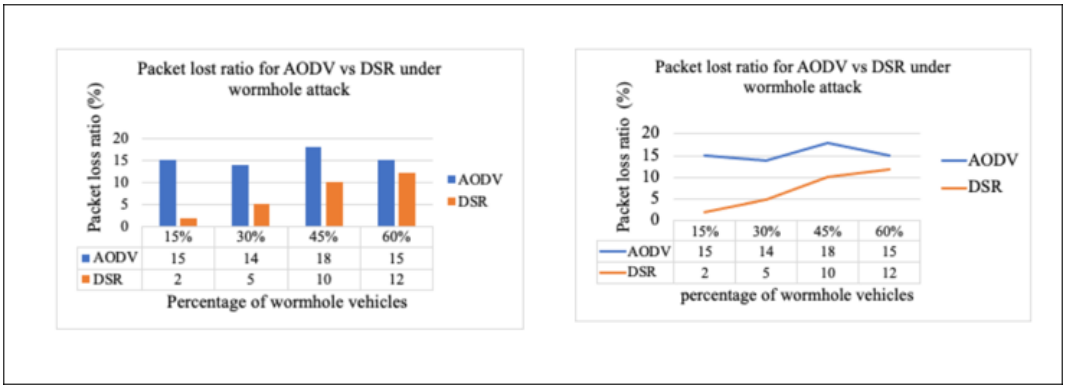

Fig.10 Packet loss ratio for AODV vs DSR under wormhole attack

8.6 Packet delivery ratio under wormhole attacks

Fig.11 shows that the packet delivery ratio for both protocols decreases with an increase in the percentage of wormhole attacks within the network. However, overall, the DSR protocol still outperforms AODV.

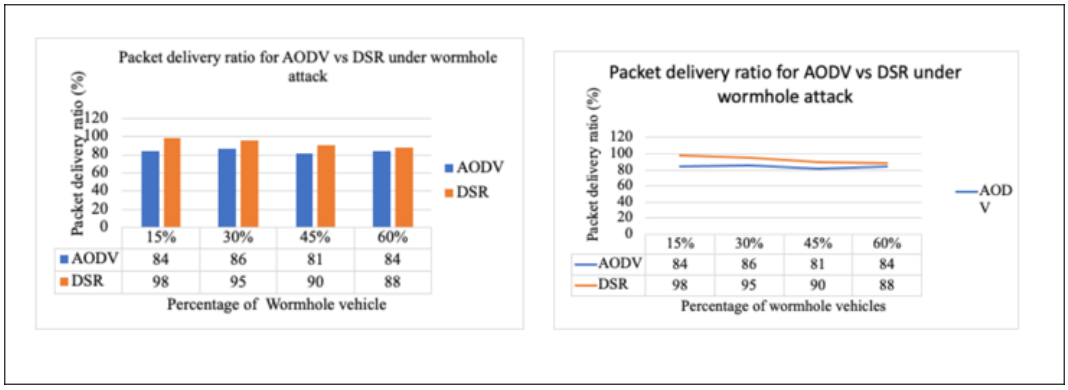

Fig.11 Packet delivery ratio for AODV vs DSR under wormhole attack

8.7 Average throughput under wormhole attacks

Fig.12 describes the average throughput for both protocols under different percentages of wormhole vehicles. The simulation results show that both protocols are affected by the increased ratio of wormhole attacks. However, AODV performs better than DSR when the percentage of attacking vehicles increases when measuring the *average throughput*.

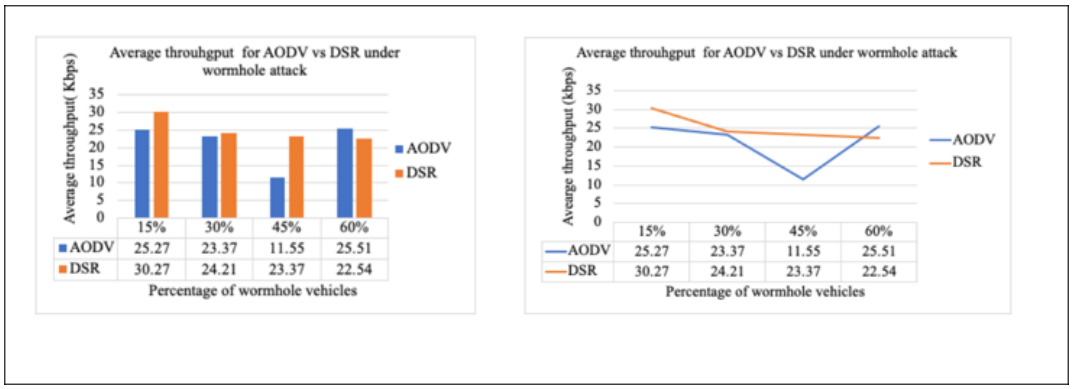

Fig.12 Average Throughput for AODV vs DSR under wormhole attack

8.8 Average end-to-end delay under wormhole attacks

Fig.13 below shows both protocols' *average end-to-end delay* under wormhole attacks. The two protocols have performed similarly when assessing the average delay metric. The average delay fluctuates with increased wormhole vehicles because the collision is reduced due to the number of dropped packets. Overall, DSR outperforms AODV in terms of *average end-to-end delay*.

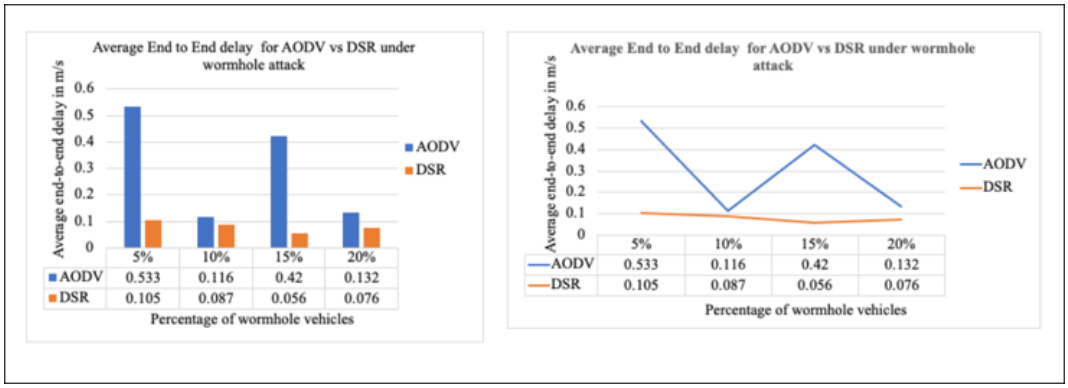

Fig.13 Average end-to-end delay for AODV vs DSR under wormhole attack

9. PROPOSED MITIGATION SYSTEM

The aim of the proposed system is to detect malicious vehicles and protect the VANETs from attacks. Malicious behaviour could happen in different ways such as packet modification, packet dropping, altering the network topology, or creating faked vehicles.

VANETs are vulnerable to several security issues and many researchers tried to find effective security techniques. For example, hard encryption security techniques provide high security to VANETs by using algorithms to encrypt and decrypt the data. VANET nodes are easy to compromise and could face a lot of misbehaviours, therefore a misbehaving vehicle may deploy different types of attacks to interrupt the network communication through a compromised node. Therefore, the proposed system, which is called the soft encryption security technique aims to detect misbehaving vehicles that act as a malicious vehicles. When the traffic transmits through the network and those misbehaving nodes act as malicious nodes, the proposed scheme will try to detect, punish, isolate and report such hostile vehicles from the network. Figure 14 represents the general framework of soft encryption security techniques. In this scheme, each vehicle in the network should observe the behaviour of its neighbours to classify them as malicious or trusted. Nodes will evaluate nodes' cooperation or defection by observing the forwarding packets' behaviour. Its neighbour nodes will monitor packets generated by each vehicle in the network. Packet forwarding is the only metric used in this study to determine which vehicle misbehaved during data transmission in the network. In this system, there are two types of the table will be created as follows:

9.1 Node Bahaviour Table (NBT)

Node Behaviour Table (NBT)In this table, each vehicle or node observes its neighbour, "direct neighbour", and builds a local trust table or node behaviour table to record the behaviour and the trust value. Then based on the node's behaviour, the decision will be taken as a regular node or malicious node.

9.2 Black List Table (BLT)

In this table, each vehicle or node in the network stores information about one hop node away. In addition, BLT contains information about each node in the network and to keep the trust schema updated, this table is distributed between neighbours.

Thus, this system keeps VANETs secure by using trust between vehicles while sending and receiving network data. If any vehicles behave as malicious, then the decision is to isolate these malicious nodes by adding them to the blacklist table. Figure 14 explains how soft encryption security techniques work based on trust values between vehicles.

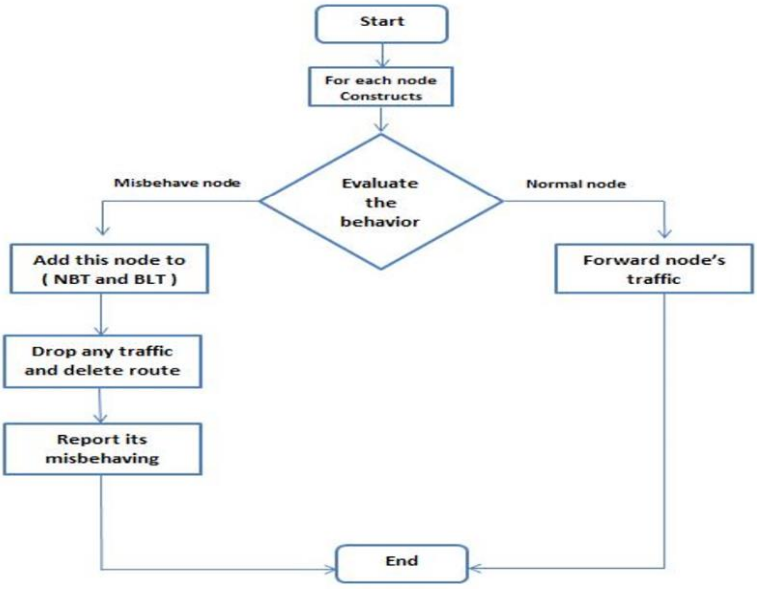

Fig.14 Flowchart of Soft Encryption

9.3 IMPLEMENTATION OF SOFT ENCRYPTION

In this scenario, network implementation includes 70 vehicles nodes operating under DSR as a routing protocol at different times of 100, 200, 300, 400, 500 seconds in three scenarios: the normal DSR in which vehicles operate in ideal conditions with normal behaviour; the malicious DSR that includes several malicious nodes ranging from 10% to 50% of nodes in the networks without security mechanism in place;

In the third scenario, the soft encryption solution is applied to the VANETs with malicious nodes to mitigate such behaviour. The proposed algorithm aims to detect misbehaving nodes, isolating them from the network and dropping their packets. On the other hand, reward the well-behaving nodes by forwarding their traffic.
The performance of the network in the three scenarios is measured using the following parameters:

9.3.1 Packet Delivery Ratio

Figure 15 shows that although the soft encryption solution does not reach the performance of the normal DSR with no misbehaving nodes, it shows an enhancement in terms of PDR rate, and DSR performs better than DSR without a security mechanism in all percentages of misbehaving nodes.

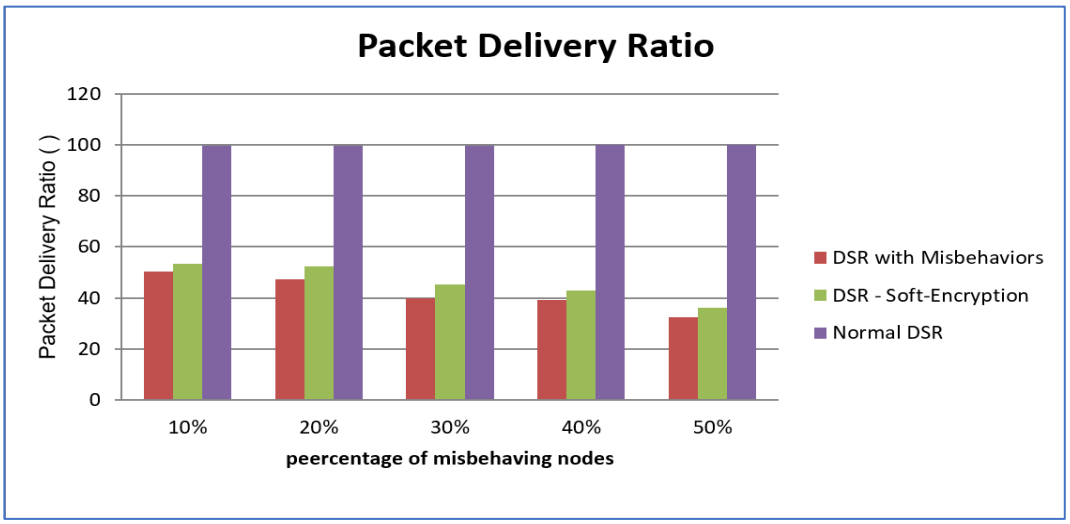

Fig.15 PDR for DRS under malicious nodes and soft encryption

9.3.2 Throughput

Figure 16 investigates throughput based on the three scenarios as in the previous figure. The throughput performance metric of the DSR with the soft encryption is better than the DSR without a security scheme. This improvement is achieved because the algorithm can help nodes mitigate the influence of misbehaving nodes. The DSR with the soft encryption performance is less than the normal DSR because nodes take some time to discover the misbehaviour of nodes. Reporting such misbehaviour is essential to help nodes find the malicious nodes before interacting with them. However, this algorithm shows promising results as the throughput nearly reaches the ideal value when 30% of misbehaving nodes are inserted in the network.

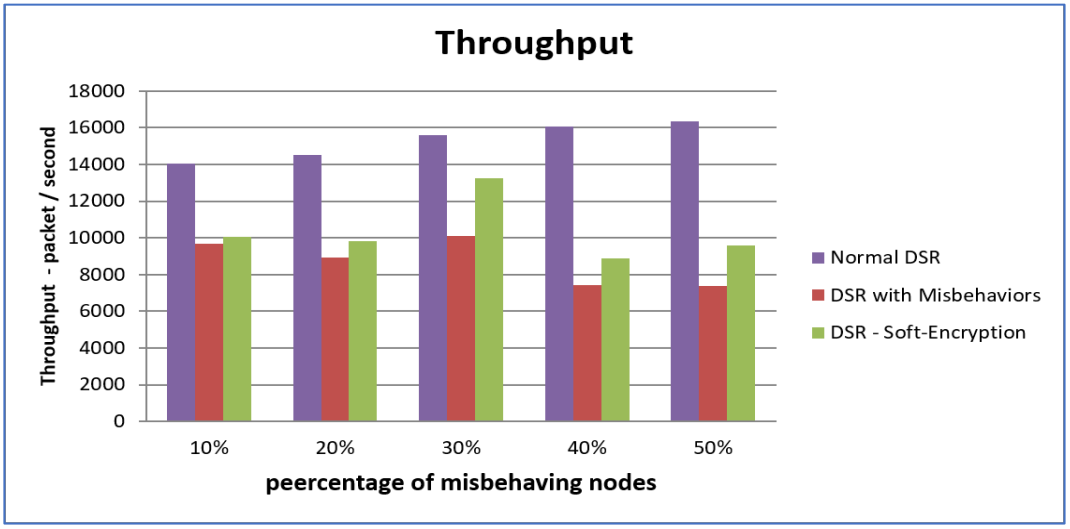

Fig. 16 Throughput of misbehaving nodes and soft encryption

9.3.3 Packets Dropped

Figure 17 shows that the DSR with a soft encryption solution performs better than the DSR without a solution for misbehaving nodes. For example, packets dropped by the DSR with soft encryption reach 5732 at the worst case when the misbehaving nodes get 50% while the DSR without the solution goes more than 6000 packets at the same percentage.

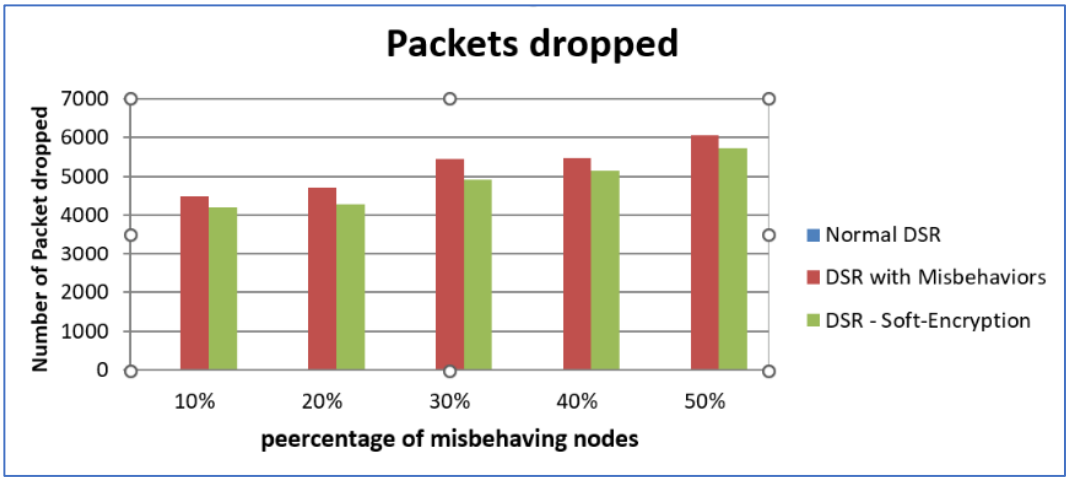

Fig. 17 Packet dropped vs misbehaving nodes and soft encryption

9.3.4 Average Delay

Figure 18 shows that the average delay is higher when applying soft encryption, especially at 30% of malicious nodes, due to the algorithm taking longer to check all the nodes in the network and dropping their packets.

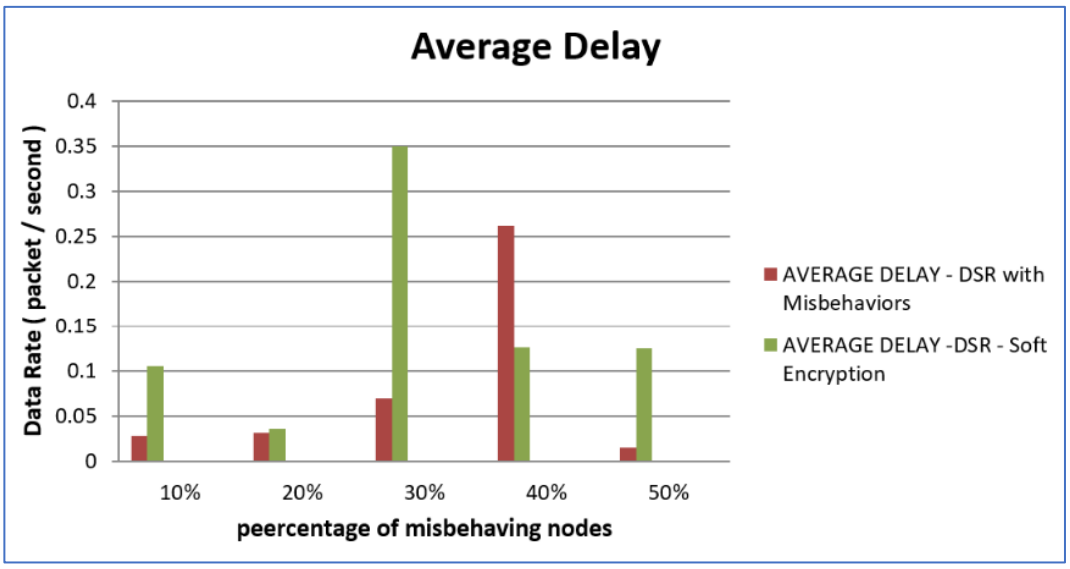

Fig. 18 Average delay vs misbehaving nodes and soft encryption

10. CONCLUSION

There are several security issues in VANET where attackers look for ways to intercept data during their exchange between vehicles within a network.
The performance of two reactive protocols (AODV and DSR) is evaluated using a network simulator. The simulation uses NS3 by measuring performance metrics such as packet delivery ratio, packet loss ratio, average throughput, and average end-to-end delay under different attacks by introducing different percentages of malicious vehicles into the network.

The results show that DSR outperforms AODV when subjecting these protocols to blackhole and wormhole attacks. However, AODV outperforms DSR when measuring the average throughput under the same attacks.
The main contribution of this research is analysing the performance of the network protocol under malicious attack and implementing a countermeasure technique called soft encryption. The proposed algorithm detects misbehaving nodes, isolates them from the network and drops their packets. On the other hand, reward the well-behaving nodes by forwarding their traffic.

The trend of attacks continues on internal vehicle communication systems and V2V communications. Therefore research and new mitigation techniques are emerging in CAN security, as well as the security of authentication protocols, intrusion detection systems and machine learning algorithms to secure future autonomous vehicles and save lives.

The limitation of this research is that the performance of the routing protocols is evaluated using only NS3 without considering the road traffic simulator capable of generating mobility traces. Therefore, for future work, I recommend using SUMO to simulate the position of the vehicles and traffic management [17].

REFERENCES

[1] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei and R. Das, "Attacks on Self-Driving Cars and Their Countermeasures: A Survey," in IEEE Access, vol. 8, pp. 207308-207342, 2020.

[2] W. Wang, F. Xie and M. Chatterjee, "Small-Scale and Large-Scale Routing in Vehicular Ad Hoc Networks," *in* IEEE Transactions on Vehicular Technology, vol. 58, no. 9, pp. 5200-5213, Nov. 2009.

[3] P. Sathya Narayanan and C. S. Joice, "Vehicle-to-Vehicle (V2V) Communication using Routing Protocols: A Review," 2019 International Conference on Smart Structures and Systems (ICSSS), 2019.

[4] T. Mantoro and M. Reza, "Performance analysis of AODV and DSDV using SUMO, MOVE and NS2," 2016 International Conference on Informatics and Computing (ICIC).

[5] A. D. Devangavi and R. Gupta, "Routing protocols in VANET — A survey," 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon), 2017, pp. 163-167.

[6] Kaur, H. (2017) "Analysis of VANET geographic routing protocols on real city map." In Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017 2nd IEEE International Conference on, pp. 895-899.

[7] Malik, Suman, and Prasant Kumar Sahu. "A comparative study on routing protocols for VANETs." *Heliyon* 5, no. 8 (2019).

[8] Karthigha, M., Latha, L. and Sripriyan, K. (2020) A Comprehensive Survey of Routing Attacks in Wireless Mobile Ad hoc Networks": 2020 International Conference on Inventive Computation Technologies (ICICT), 2020.

[9] A. M. Yassin and M. A. Azer, "Performance Comparison of AODV and DSDV In Vehicular Ad Hoc Networks," 2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC), *2022.*

[10] Ajay N. Upadhyaya and J.S.Shah. "Effect on AODV Routing Protocol under Blackhole Attack in VANET," 2019 International Journal of Computer Engineering and Technology (IJCET), Volume 10, Issue 3, May-June 2019, pp. 166-174.

[11] Richhriya, V., Maurya, J.P. and Saxena, T. "Performance of AODV against Malicious node in Mobile Ad Hoc Network," International Journal of Engineering in Current Trends (IJERCT), Volume-2, Issue-3, June 2020.

[12] Siddiqui, M.N., Malik, K.R. and Malik, T.S. "Performance Analysis of Blackhole and Wormhole Attack in MANET Based IoT," 2021 International Conference on Digital Futures and Transformative Technologies (ICoDT2), 2021.

[13] R. Mena, F. Zumárraga, L. Urquiza and X. Calderón, "Google Maps Route Color Mapping with SUMO Simulator," 2019 International Conference on Information Systems and Software Technologies (ICI2ST), *2019*

[14] Gorine and Saleh, R. (2019) Performance Analysis of Routing Protocols in MANET Under Malicious Attacks. International Journal of Network Security & Its Applications.

[15] A. U. Khan, M. D. Chawhan, M. M. Mushrif and B. Neole, "Performance Analysis of Adhoc On-demand Distance Vector Protocol under the influence of Blackhole, Gray-Hole and Wormhole Attacks in Mobile Adhoc Network," *2021* 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2021, pp. 238-243.

[16] Chaudhary, R., Sethi, S., Keshari, R., and Goel S. (2012) "A study of Comparison of Network Simulator-3 and Network Simulator-2." International Journal of Computer Science and Information Technologies, 3(1).3085-3092.

[17] A. M. Shaban, S. Kurnaz and A. M. Shantaf, "Evaluation DSDV, AODV and OLSR routing protocols in real live by using SUMO with NS3 simulation in VANET," 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2020, pp. 1-5,

[18] S. Iqbal, P. Ball, M. H. Kamarudin and A. Bradley, "Simulating Malicious Attacks on VANETs for Connected and Autonomous Vehicle Cybersecurity: A Machine Learning Dataset," 2022 13th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP*)*, Porto, Portugal, 2022, pp. 332-337.