SAKARYA UNIVERSITY JOURNAL OF COMPUTER AND INFORMATION SCIENCES
VOL. 5, NO. 3, DECEMBER 2022
DOI: 10.35377/saucis.05.03.1175613

Research Article

FA-AODV: Flooding Attacks Detection Based Ad Hoc On-Demand Distance Vector Routing Protocol for VANET

Bugra Alp Tosunoglu[1], Cemal Kocak[2]
[1]Department of Computer Engineering, Faculty of Technology, University of Gazi, balp.tosunoglu@gazi.edu.tr,
06500, Ankara, Turkey
[2]Department of Computer Engineering, Faculty of Technology, University of Gazi, ccckocak@gazi.edu.tr,
06500, Ankara, Turkey

Received 15 September 2022; Revised 9 October 2022; Accepted 24 October 2022; Published online 31 December 2022

Abstract

Vehicular Ad-Hoc Networks (VANET) is anticipated to be the most effective way of increasing performance and safety in transportation soon. VANETs are the sub-branch of Ad-Hoc Networks which provide safety and comfort features together with related services for the vehicle operators. RREQ flood attack mostly encountered in the literature for security of VANET. Due to the nature of the reactive protocols, the AODV routing protocol is quite open to attack types such as flood attack. Flood attacks occur in the network layer. The impact of flood attacks is not about victim nodes, it can be also affecting the whole network. A malicious attack that could be carried out in VANET could cause accidents that would cause a serious disaster. A malicious node could penetrate the IP addresses on a Flood Attack based User Datagram Protocol (UDP) to breakdown the data communication between two vehicles. The main purpose of this paper is to detect and prevent the flood attack, during the operation of the routing protocol and to decrease the end-to-end delay on the network.

Keywords: Vehicular AdHoc Networks, VANET Security, Flooding Attack, NS2

1. Introduction

Wireless networks made up of mobile nodes behaving arbitrarily and lacking infrastructure are known as mobile ad-hoc networks (MANET). There is no specified central control, such as a base station, in these kinds of networks. Another variant of MANET is the vehicular ad-hoc network (VANET), which is a more recent technology. Wireless communication between cars and between vehicles and the Roadside Unit (RSU) is made possible via VANET [1].

A group of engineers from IBM Cooperation and Delphi Delco Electronic Systems initially proposed the VANET. This team claims that the Inter-Vehicle Communication (IVC) and Roadside to Vehicles Communication (RVC) systems of vehicle communication are together referred to as VANET. VANET technology utilizes both cellular networks and Ad-Hoc Networks for maintain a connection. The infrastructure of the VANET, on the other hand, consists of a hybrid design that combines VLAN/Cellular, Ad-Hoc, and vehicular communications (V2V, V2I, and V2R). It is acknowledged that VANET is a part of the Intelligent Transport Systems (ITS). ITS facilitates communication amongst other vehicles by utilizing their safety and service applications [2-4]. VANET routing protocols, most notably as AODV and DSR, help create a route between the source node and the destination node. These routing protocols are divided into three main classes: proactive, reactive and hybrid.

For each route entry, the AODV protocol employs the destination sequence number; this sequence number provides a loop-free connection and the shortest way. This RREQ message is forwarded by the other mobile node after being propagated from the source. This message is subsequently transmitted to the intermediate node's neighboring node. This process is repeated until the packet reaches the destination or central node. The route entry in the routing table must be a legitimate entry, which implies that the item in the table must be less than a certain value. The hop count at the intermediate node is incremented by one as the RREQ packet moves across the network. If the node receives another RREQ message with the same ID, the packet is dropped. When an intermediate node or destination receives an

RREQ message and has a new valid route to the destination, it generates an RREP route reply message and sends it in response to the RREQ message [5].

The main purpose of the flood attacks is to consume the resources of the assets on the network. This type of attack is the category of large routing distortion that can lead to denial of service. Flood attacks occur in the network layer. The attacker continuously sends a RREQ message to the selected node. To respond to any incoming request, specific resources are allocated to the attacker by the target node. This behavior causes the destination node to run out of resources. IP address spoof-based flood attacks are a serious and still open security issue in wireless networks. IP address spoofing creates offensive fake routing packets using addresses that are assigned to others or never assigned. Several security solutions have been proposed to solve various problems related to flood attacks in the VANETs [6-8].

Our main goal is to provide secure and fast communication between the source node and the destination using the AODV protocol. We would like to give a suggestion that we limit to a solution for the detection and prevention of RREQ message type flood attacks. This proposed mechanism identifies not only the attack but also the source of the attack and isolates the attacker from the network. With proposed mechanism, end-to-end delays, and count of dropped packages will reduce, and the number of transmitted packets will increase.

The rest of this paper is organized as follows. In Section 2, related works on background of flood attack types on VANET and special subsection for flooding attack are mentioned. Section 3 describes the proposed FA-AODV. Section 4 presents the simulation parameters and performance metrics. The performance of FA-AODV is evaluated and compared with the default AODV as well as in Section 4. Section 5 draws the conclusions.

2. Related Work

In section definition of flood attack in AdHoc networks and previous studies on the type of floods that are subject to the study are discussed.

Flood Attack: Because reactive routing packets, such as AODV and DSR, set the route by using a route request, dependence on RREQ packets makes the reactive protocols vulnerable to flood attacks. RREQ flood attacks or data flood attacks depend on packets used on the network. The purpose of the malware node in RREQ flood attacks is to generate a flood of data by sending many RREQ packets of unknown targets on the network. If the target nodes are not present in the network, RREP packets will not be created, but RREQ packets will continue to be created by all nodes. The purpose of this type of attack is to consume bandwidth and network resources.

2.1. Flood Attacks In VANET

Using two well-known frameworks in uncertain reasoning, namely Bayesian Inference and Dempster-Shafer (D-S) evidence theory, innovative strategies for resisting RREQ flooding attacks in Wireless Ad Hoc Networks were proposed [9]. The current study describes the modeling of RREQ traffic and the development of an optimal method for detecting persistent RREQ flooding attacks using Bayesian Inference. Using D-S evidence theory, the method was further developed to identify high and low rate pulsed RREQ flooding attacks. The suggested solution effectively resisted any sort of flooding-based DDoS attack in Wireless Ad Hoc Network with decreased communication and memory cost, according to a detailed assessment utilizing mathematical modeling and simulation.

Al-Mehdhara et al [10], propose a secure VANET architecture that makes use of a Software-Defined Networking (SDN) controller and Neural Network Self-Organizing Maps (SOMs). A Multilayer Distributed SOM (MSOM) model based on two levels of clustering and classification is used to address the shortcomings of traditional SOMs and improve SOM efficiency. Experiment findings reveal that malicious traffic is detected at 99.67%, DDoS attacks are prevented, and system security is increased.

Another SDN study, have proposed the recognition of DDoS attacks to SD-VANET based on a combination of Hyperparameter optimization and feature selection. Initially, created a dataset containing both the characteristics of normal network traffic and DDoS attack network traffic was obtained from SD-VANET topology. Minimum Redundancy Maximum Relevance (MRMR) feature selection algorithm was used to select the most distinctive features of the dataset. Bayesian optimization method boosted with hyperparameter optimization was applied using for classifiers in the learning phase. The best accuracy score attained using MRMR feature selection and Bayesian optimization-based decision tree classifier was 99.35% [11].

Zarei et al. [12], presented the LSFA-IoT strategy, which protects the AODV routing protocol as well as the IoT network against flooding. The authors divided the project into two major phases: the first involves identifying attackers using a physical layer intrusion and attack detection system, and the second involves detecting wrong events using Average Packet Transmission RREQ (APT-RREQ) messages. The simulation results demonstrated that the suggested technique outperformed the well-known IOT protocols REATO and IRAD.

The authors compared different ML approaches to detect malicious activity and the proposed Hybrid KSVM algorithm for DDoS attack. Their Hybrid KSVM algorithms gave better results with accuracy (92.46%) and precision (95.31%) compared to other ML algorithms [13].

The authors [14] worked on Information-centric networking (ICN)-based Named Data Networking (NDN), which they believe is the future of the internet in autonomous or semi-autonomous vehicles. NDN-based VANET suffers from several security attacks, one such attack is the Interest Flood Attack (IFA), which targets the core routing mechanism of NDN-based VANET. Their suggested approach can identify both normal and low-rate IFA. The results of their experiments reveal that their technique detects and mitigates both regular and low-rate IFA in the network.

Hasan et al. [15] proposed the FLOW-AODV algorithm for detecting the flood type attack when the IP address of the attacker was hidden. The smaller average delay in FLOW-AODV, as supported by the simulation results, means that it prevents redundant RREQ overflow from frequent flooding. In addition, results based on the appearance of multiple flood attackers' algorithm maintain almost 100% PDR with less than 200 ms. delay.

3. Material and Methods

3.1. FA-AODV Algorithm and Simulation Styling

In this study, prevention of UDP flooding type attacks made on the AODV protocol is used in VANET for providing the continuation of the communication. For this, an algorithm named Flooding Attacks detection based Ad Hoc On-Demand Distance Vector Routing Protocol (FA-AODV) has been developed. As is known, AODV protocol works on demand. As the nodes are in mobility, the road information keeps changing continuously. For this reason, during the route discovery process, every node between the source and the destination nodes decides to either relay or drop the RREQ packets. In the scenario, attacks are realized using RREQ packets. During the attack number of packets given in the table, one is triggered by all the nodes simultaneously. Thus, the blockage of the network and prevention of the communication will be ensured.

Table 1 Number of UDP flooding attack packets triggered

Number of UDP Flooding Attacks Packet				
	20 Node	***15 Node***	***10 Node***	***5 Node***
Std. AODV	11339	10081	4449	3646
FA-AODV	9445	8135	5385	3221

Flood attacks are performed using UDP or ICMP packets. In these types of traffic types, in which the SYNC mechanism would not work, the attacker sends UDP packets to randomly or previously chosen ports. The attacked nodes investigate every packet that arrives to understand the services requested. This situation would decrease the performance in nodes that is; it increases the end-to-end delays. The attacked node would check the availability of the port assigned for the incoming request and by concluding no ports are in listening state, it would be forced to send “Destination Unreachable” messages. These unlimited numbers of packets are processed. This situation would cause the data traffic it has with the neighboring nodes to be stopped. As a result of this attack, it would cause the victim node to be unreachable by the other nodes.

In figure 1, flow diagram for FA-AODV algorithm has been displayed. According to flow diagram and hypothetical scenario, all nodes on the network listen to packet communication of other neighbor nodes by working in “promiscuous mode”. On realizing next node exceeds previously defined packet drop threshold level, that node is identified as hostile. This related node will not be used for the next packet traffic.

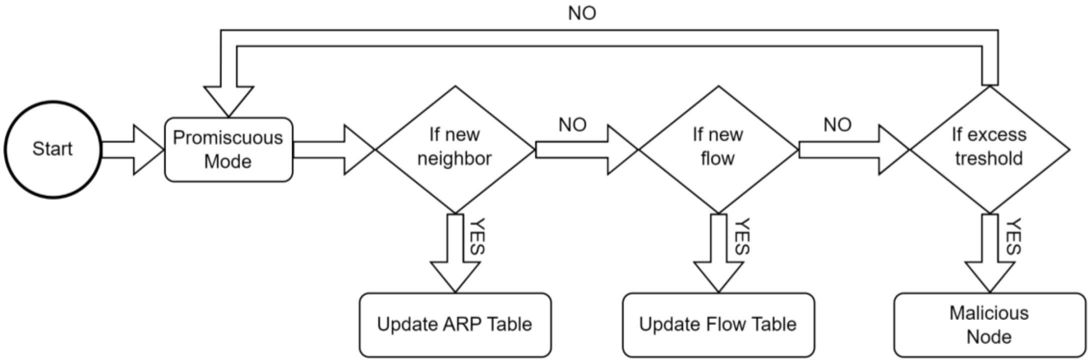


Figure 1 Flow Diagram for FA-AODV

A pseudo code developed for the FA-AODV algorithm is shown in pseudo code 1.

Code 1 FA-AODV Pseudo Code

```
Begin
 If the sender / receiver listens to the data packet
  Begin
   If the expected packet
    Begin
     Deliver packet
     Condition (node) = good
    End
   If the sender's packet timed out
   Begin
    If (forwarded packet)> threshold value
    Begin
     If Condition (node)! = Good
      Begin
        Generate Alarm to Source
        Condition (Node) = Malicious
    End
   End
  End
 End
End
```

According to the pseudo code and the hypothetical scenario, algorithm to benefit of “promiscuous mode”. All nodes on the network listen to packet communication of other neighbors. When the next node exceeds threshold level, which is previously defined, that node is identified as malicious. Malicious node won’t be used for the next traffic. Identifier nodes send a broadcast message to other nodes in neighbors to a malicious node and drops the packet. It will mark the source node as an attacker, and it will drop the packets coming from the same source. If it is a standard packet, it will send an RREP packet and route initiation process will be started.

Thanks to the FA-AODV algorithm developed, with the dropping of RREQ packets sent in a flooding attack type with a purpose to determine a route, the malicious attacks have been prevented and network congestion has been removed at the same time. Thus, the regional blockage and the communication breakdown targeted by the attacker have been prevented. The ratio of the number of packets sent by the source node to the number of packets received by the destination node is described as data flow. With the FA-AODV algorithm suggested in present study, it is aimed that the data flow rate is increased. As the flow rate increases, recovery has been achieved in the average end-to-end delay.

3.2. Realized Simulation

NS-2 simulation involves many applications, protocols, network types, and network element and traffic model. NS-2 is an object-based simulator which Coded in C++. Object oriented extension of Tool command language (OTcl) will be used from Ns2 for interpreter to run user scripts during simulation. OTcl scripts help users to define detailed network topologies, to simulate featured protocol and applications, and to retrieve simulation results in a specific format. It has been developed by TCL Jhon Ousterhout and has emerged as a language suitable for fast development, able to supply graphic interface, compatible with many platforms and easy to use [17, 18].

In this study, network planning has been performed using the algorithms of the standard AODV and the FA-AODV developed according to the parameter values given in Table 2 on the NS-2 network simulator.

Table 2 Simulation parameters value

Parameters	**Values**
Channel	Wireless
Propagation	Two Ray Ground
Mac Protocol	802.11
Routing Queue	Queue Drop tail
Antenna	Omni Antenna
Energy Model	Battery
Simulation area (m)	1000*1000
Number of nodes	5, 10, 15, 20
Simulation stop time	6s
Mobility	20 - 25 m/s
Traffic type	CBR
Attacks type	UDP floods
Number of flood node	1, 2, 3, 4

Randomly chosen 5, 10, 15 and 20 nodes, distributed in the overall of the simulation domain given in Table 2 were generated. The speeds of the nodes are assigned with a speed of 0-25 m/s. The assigning of the speeds in this range is done randomly. For it to make sense, the running time is set to 2.5 m/s. The source and the destination packets were defined and the times at which the communications would start, and stop were specified in the TCL file. The nodes (vehicles) make communications as per the conditions stated in TCL configuration table. As of the 0,25th second of the simulation, the vehicles take off for different coordinates at 15-25 m/s speeds. To capture the destination node, UDP flooding attacks are initiated at the 0-1,5 seconds of the simulation using a CBR traffic over UDP traffic. At the 0-1 seconds of the simulation, the node2 (Vehicle numbered 0) is captured by attackers. Then, at the 1 second, flooding type attacks are started over Node2 as shown in Figure 2.

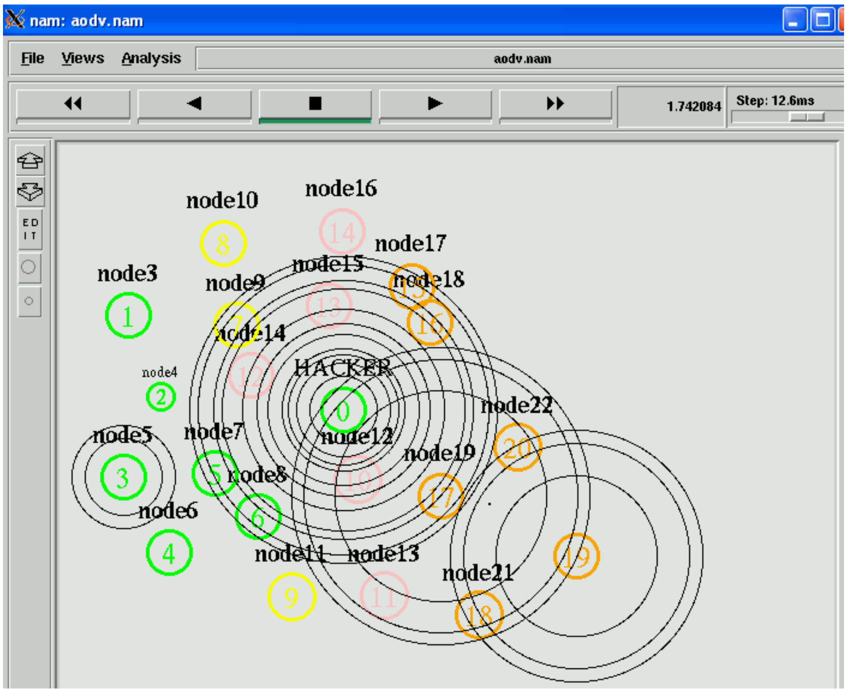
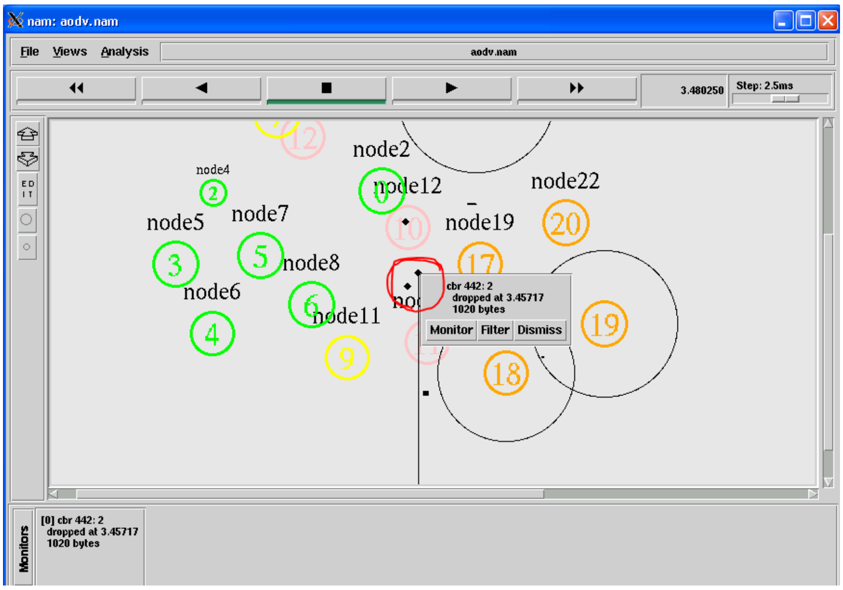


Figure 2 Malicious broadcast of Node2 to other nodes with a flood attack.

At the 1 – 2,5 seconds interval of the simulation, the dropped packets due to the algorithm that comes into play after the flood attacks performed are shown in Figure 3.



cbr 442: 2
dropped at 3.45717
1020 bytes

[0] cbr 442: 2
dropped at 3.45717
1020 bytes

Figure 3 Dropped Packets

4. FA-AODV Algorithm Performance Analysis

To evaluate the results of the suggested algorithm, simulation of two different models were run. The first of them is the implementation of UDP flooding attacks on the AODV protocol used in VANET. The second one is the simulation of the model in which the suggested FA-AODV algorithm is used. For both models, 5, 10, 15 and 20 nodes were used. There is one malicious node for five nodes (5-1, 10-2, 15-3, and 20-4). For performance criteria, the end-to-end average delay containing all the possible delays resulting from the queuing during the route discovery process, total of dropped packets and the number of packets that reached the destination in data transfer were compared.

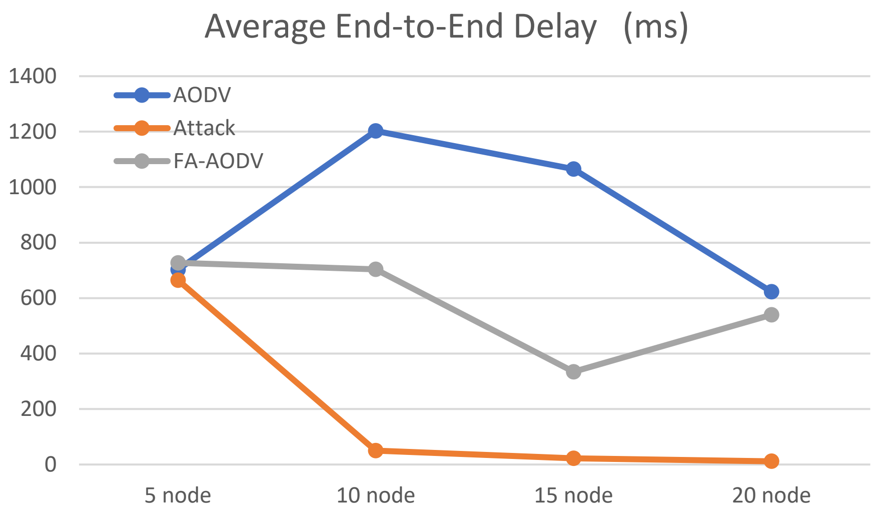


Figure 4 Average end-to-end delay

When the end-to-end average latency is examined, as seen in Figure 4, in the scenario which has 5 nodes, the delays between the scenarios are very close because of the distance between the vehicles. As the number of nodes under attack increases, average end-to-end reduces from the attacker node to the neighbor nodes because the packet transmission is too high. The proposed FA-AODV algorithm showed less latency compared to the standard AODV algorithm.

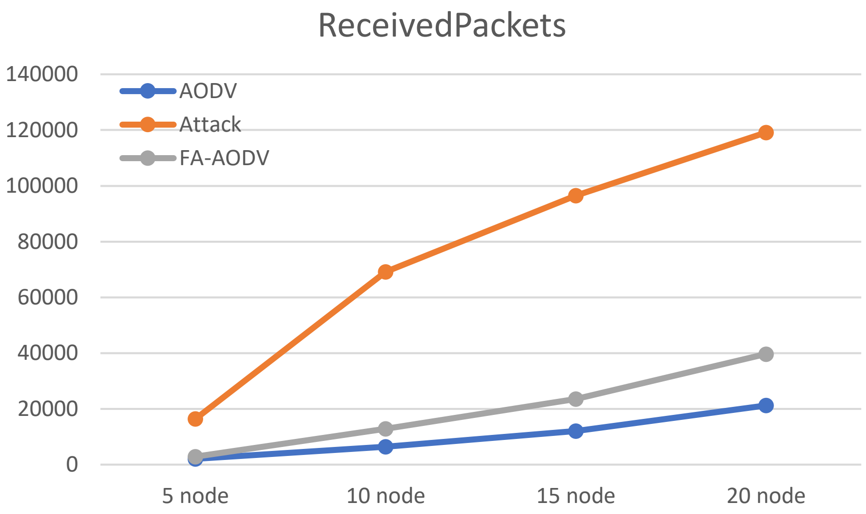


Figure 5 Received packets

The number of packets received by the attacked vehicles is given in figure 5. In the scenario where the standard AODV algorithm is used under attack, more packet reaches the target with the increase of attacker nodes. However, in the FA-AODV scenario, although the number of aggressors increased, results were very close to the non-attacked AODV scenario. In this way, fewer and safer packets were delivered to the target.

The studies in the literature were examined with the proposed method in terms of average end-to-end delay. The proposed method has provided less end-to-end delay times than [15,16]. The studies in the references [6,8] show a high similarity with the proposed method in terms of end-to-end delay times

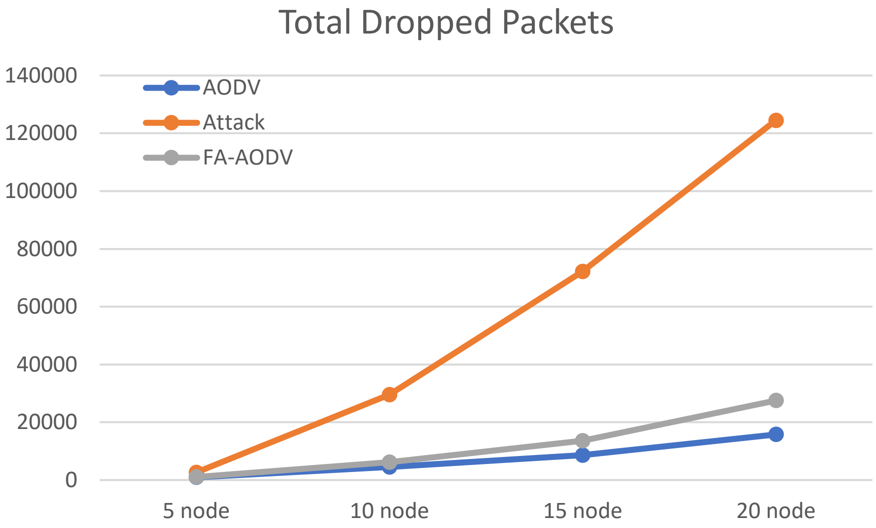


Figure 6 Dropped packets in total

In Figure 6, the comparison of the dropped packets uses the proposed FA-AODV algorithm instead of the attacked AODV protocol, and results obtained are close to the AODV protocol which works in the non-attack scenario due to isolating the attacker nodes from the network. The increase in the number of packets dropped indicates that the attacker blocked the communication and caused a network blockage. In the 5-nodes 1 attacker scenario, 2642 packets are dropped, while in the 20-node 4-attackers scenario, 124507 packets are dropped.

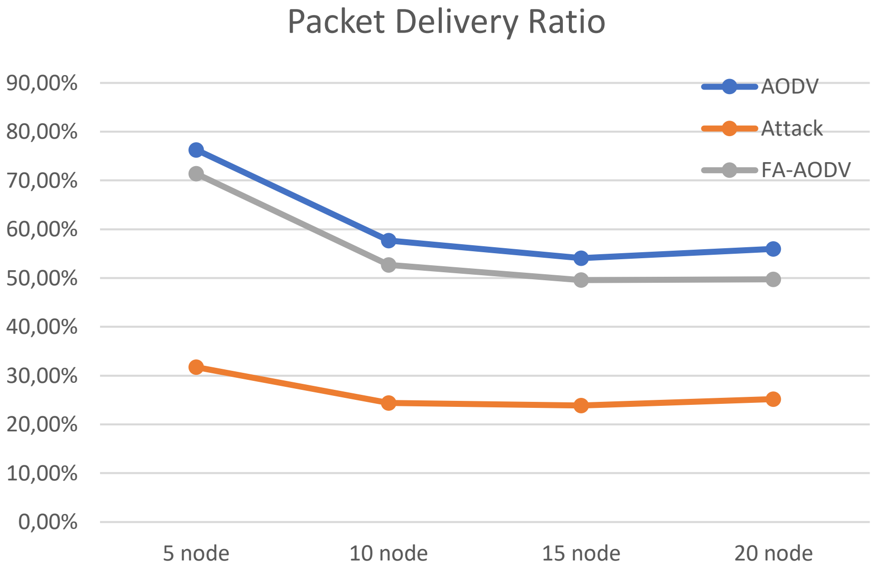


Figure 7 Packet Delivery Ratio

The Packet Delivery Ratio is another metric indicating the network quality. In the AODV protocol running under attack, packet transmission rates are reduced to 30%. As seen in Figure 7, the results of FA-AODV algorithm were close to the standard AODV algorithm results.

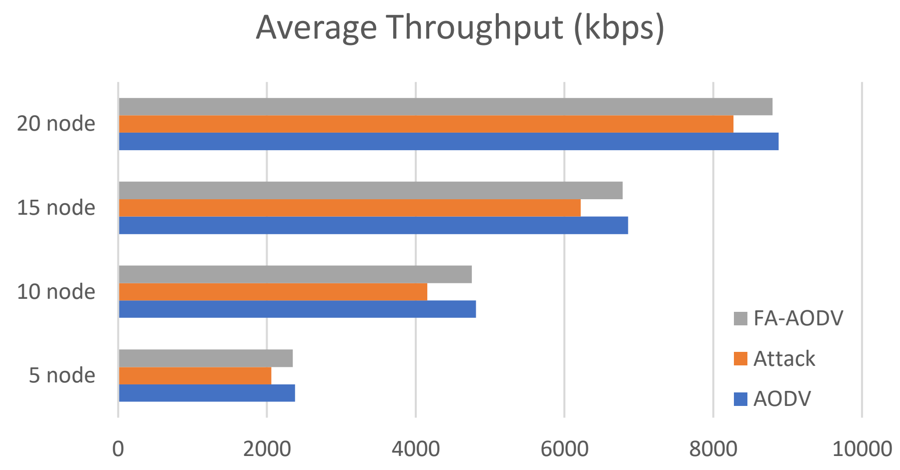


Figure 8 Average Throughput

The average throughput given in Figure 8 refers to the average data rate of successful data or message transmission over the connection. (Received Size / (Stop Time-Start Time)) * (8/1000). When the average throughputs were examined, it was observed that the FA-AODV algorithm results were close to the non-attack AODV algorithm results, due to packet transmission with under attack.

Table 3 Routing Load

Routing Load	AODV	Attack	FA-AODV
5 nodes	0,025	6,982	0,265
10 nodes	0,23	142,545	1,427
15 nodes	0,646	363,824	2,989
20 nodes	2,068	978,458	7,771

As can be seen in Table 3, the load of the network under attack increases exponentially as the number of nodes increases. This also seen in Figure 9 The FA-AODV algorithm has improved the network load when network is under attack.

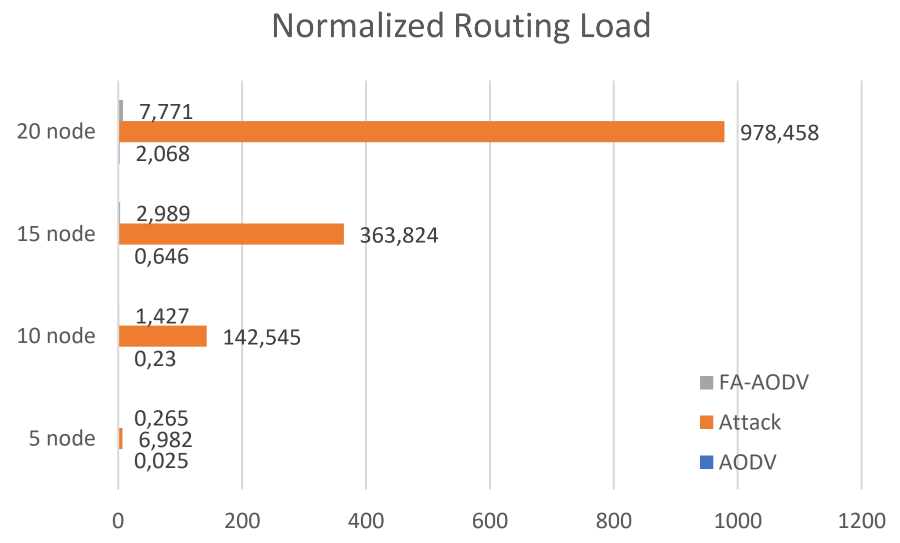


Figure 9 Routing Load

5. Conclusion

In this study, the FA-AODV algorithm that prevents UDP flooding type attacks made on the AODV protocol is used in VANET. The results are compared using two models, which are standard AODV and FA-AODV. For the performance analysis, average end-to-end delay, received packets and total dropped packets have been used. The FA-AODV algorithm checks the hop count and packet IDs in the RREQ packets and decides whether it is an attack or not. It has ensured the continuity of the communication by dropping the attacking packets. Therefore, the FA-AODV algorithm has not produced traffic load by preventing the network from getting congested. Despite the attacks, the performance of the moving nodes has been increased and continuation of a safe communication has been ensured. Therefore, FA-AODV algorithm prevents the UDP flooding type attacks and provides faster and safer communication. Safer communication has been established and the packets have been sent to the destination in the shortest time possible. Considerable improvements have been achieved in the average end-to-end delay and number of packets delivered. As it is considered that the attackers could conduct different types of attacks on the network, it is suggested that the algorithm be improved against the types of attacks apart from flooding. For the future work, we will plan to compare the proposed FA-AODV algorithm with other reactive routing protocols (DSR, TORA etc) used in VANET.

References

[1] S.-H. Kim and I.-Y. Lee, “A Secure and Efficient Vehicle-to-Vehicle Communication Scheme using Bloom Filter in VANETs,” *International Journal of Security and Its Applications*, vol. 8, no. 2, pp. 9–24, Mar. 2014, doi: 10.14257/ijsia.2014.8.2.02.

[2] M. Y. Gadkari, “VANET: Routing Protocols, Security Issues and Simulation Tools,” *IOSR Journal of Computer Engineering*, vol. 3, no. 3, pp. 28–38, 2012, doi: 10.9790/0661-0332838.

[3] N. Arulkumar and E. G. D. P. Raj, “A simulation based study to implement Intelligent Transport Systems concepts in VANETs using AODV routing protocol in NS2,” *2012 Fourth International Conference on Advanced Computing (ICoAC)*, vol. 1, no. 1, Dec. 2012, doi: 10.1109/icoac.2012.6416854.

[4] J. Zhang, “Trust Management for VANETs,” *International Journal of Distributed Systems and Technologies*, vol. 3, no. 1, pp. 48–62, Jan. 2012, doi: 10.4018/jdst.2012010104.

[5] A. Kumar and M. Sinha, “Design and analysis of an improved AODV protocol for black hole and flooding attack in vehicular ad-hoc network (VANET),” *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 4, pp. 453–463, May 2019, doi: 10.1080/09720529.2019.1637151.

[6] M. J. Faghihniya, S. M. Hosseini, and M. Tahmasebi, “Security upgrade against RREQ flooding attack by using balance index on vehicular ad hoc network,” *Wireless Networks*, vol. 23, no. 6, pp. 1863–1874, Apr. 2016, doi: 10.1007/s11276-016-1259-2.

[7] VarshaGharu, M. Pawar, and J. Agarwal, “A literature survey on security issues of WSN and different types of attacks in network,” *Indian Journal of Computer Science and Engineering*, vol. 8, no. 2, Apr. 2017.

[8] M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi, and D. Gaiti, “Flooding attacks detection in MANETs,” *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, vol. 1, no. 1, Aug. 2015, doi: 10.1109/ssic.2015.7245675.

[9] G. S. Ganpat Joshi , “A Novel Statistical Adhoc On-Demand Distance Vector Routing Protocol Technique Is Using for Preventing the Mobile Adhoc Network from Flooding Attack,” *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 6, pp. 1753–1765, Apr. 2021.

[10] M. Al-Mehdhara and N. Ruan, “MSOM: Efficient Mechanism for Defense against DDoS Attacks in VANET,” *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, pp. 1–17, Apr. 2021, doi: 10.1155/2021/8891758.

[11] J. Rabari and A. R. P. Kumar, “FIFA: Fighting against Interest Flooding Attack in NDN-based VANET,” Jun. 2021. doi: 10.1109/iwcmc51323.2021.9498767.

[12] M. Türkoğlu, H. Polat, C. Koçak, and O. Polat, “Recognition of DDoS attacks on SD-VANET based on combination of hyperparameter optimization and feature selection,” *Expert Systems with Applications*, vol. 203, no. 1, p. 117500, Oct. 2022, doi: 10.1016/j.eswa.2022.117500.

[13] S. M. Zarei and R. Fotohi, “Defense against flooding attacks using probabilistic thresholds in the internet of things ecosystem,” *Security and Privacy*, vol. 4, no. 3, Feb. 2021.

[14] N. Kadam and K. R. Sekhar, “Machine Learning Approach of Hybrid KSVN Algorithm to Detect DDoS Attack in VANET,” *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 7, 2021, doi: 10.14569/ijacsa.2021.0120782.

[15] M. R. Hasan, Y. Zhao, Y. Luo, G. Wang, and R. M. Winter, “An Effective AODV-based Flooding Detection and Prevention for Smart Meter Network,” *Procedia Computer Science*, vol. 129, no. 1, pp. 454–460, 2018, doi: 10.1016/j.procs.2018.03.024.

[16] K. Saravanan and J. Vellingiri, “Defending MANET against flooding attack for medical application,” *2017 2nd International Conference on Communication and Electronics Systems (ICCES)*, vol. 1, no. 1, Oct. 2017, doi: 10.1109/cesys.2017.8321328.

[17] E. Altman and T. Jiménez, “NS Simulator for Beginners,” *Synthesis Lectures on Communication Networks*, vol. 5, no. 1, pp. 1–184, Jan. 2012, doi: 10.2200/s00397ed1v01y201112cnt010.

[18] “The Network Simulator - ns-2,” *Isi.edu*, 2020. https://www.isi.edu/nsnam/ns/ (accessed Sep. 14, 2022).