International Journal of Intelligent Computing and Technology

ISSN: 2457-0249 (Online)

Website: https://www.ijict.com January (2020) - Vol. 3, Iss.2 Pages:01-15

Secured AODV Routing Protocol to Improve Security in VANET

WubishetGirmaMekonnen, Nedumaran Arappali

Department of Electrical and Computer Engineering,

Kombolcha Institute of Technology-Wollo University, Ethiopia

Article History- Received: July 2019; Published: September 2019

Abstract

Vehicular ad hoc networks (VANETs) are becoming promising and popular technologies in the recent intelligent transportation world. They are used to provide an Intelligent Transportation System (ITS), efficient Traffic Information System (TIS), and Life Safety. This kind of networks is very susceptible to adversary's malicious attacks, due to the dynamic changes of the network topology, trusting the nodes to each other, lack of fixed substructure for the analysis of nodes behaviors and constrained resources. One of these attacks is black hole attack. In this attack, malicious nodes inject fault routing information to the network and lead all data packets toward themselves, then destroy them all. In this paper, we propose a solution, which enhances the security of the Ad-hoc On-demand Distance Vector (AODV) routing protocol to encounter the black hole attacks. Our solution avoids the black hole and the multiple black hole attacks. The simulation results using the Network Simulator NS2 shows that our protocol provides better security and better performance in terms of the packet delivery ratio than the AODV routing protocol in the presence of one or multiple black hole attacks with a marginal rise in average end-to-end delay and normalized routing overhead.

Keywords: Vehicular Ad Hoc networks, AODV routing protocol, security, Black hole attack

1. Introduction

Recently, because of a high number of road accidents and with the improvement in the wireless communication technologies and Vehicular Ad hoc Network (VANET) are used to provide an efficient Traffic Information System (TIS). According to the National Highway Traffic Safety Administration (NHTSA), vehicle-to-vehicle (V2V) communication has a high lifesaving potential that addresses approximately 80 percent of multi-vehicle crashes. [1]. VANET is a subclass of Mobile Ad-hoc Network (MANET) which consists of several nodes (vehicles) communicating with each other without a fixed infrastructure [2]. However, compared to MANET due to the high mobility of vehicles, VANET has an extremely dynamic topology.

The nodes tend to move in an organized pattern [3]. Besides VANETs have a potentially large scale which can comprise many participants and the capacity to extend over the entire road network [4]. Therefore, Lack of centralized management in VANET puts extra responsibilities on vehicles. Hence each vehicle is a part of the network and also manages and controls the communication on that network. The links between vehicles connect are and disconnect very often which makes routing process challenging due to the high mobility of nodes. Hence, many researchers have focused on routing in VANET. Which aims to aim to maximize the Packet Delivery Ratio (PDR) and throughput while minimizing packet loss ratio and controlling overheads.

In this direction many routing protocols have been proposed which has an important role in organizing the network safety. However, ad hoc routing protocols can be divided into reactive, proactive and hybrid protocols [5], reactive protocols do not periodically update the routing information. It finds the route only when needed like Ad Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR). Proactive protocols are typically table-driven. Destination Sequence Distance Vector (DSDV), Global State Routing GCR are examples of this type.

2. RELATED STUDIES

Black Hole detection has been an active area of research and many solutions have been proposed. However, most of and requires high overhead to detect solutions that have been proposed for MANETs that can be implemented in VANET. This section discusses some of these works.

In[10], the authors proposed an approach to detect black hole nodes in the MANET. In the proposed method, the detecting node calculates the ratio of the number of packets dropped to a total number of packets forwarded successfully. This ratio is checked with a predefined threshold value to detect any malicious behavior. If any misbehavior is found, the detecting node tries to avoid the misbehaving node.

The authors in [11] proposed a scheme (so-called DCBA) to identify and mitigate black hole/collaborative black hole attacks in MANETs. In their proposed method, each node has its

suspicious value, which is based on the abnormal difference observed between the routing messages transmitted from the node. Furthermore, when the source node receives the route reply (RREP) packet in reply to the route request (RREQ) packet, they verify the suspicious value of the node that initialized the RREP packet.

As verification, if this value is higher than the threshold level, then the node is considered as malicious and its address is stored in a blacklist table, preventing that node to further participate in the routing process.

The proposed method in [12] projects a novel automatic security mechanism using Support Vector Machine (SVM) to defend against malicious attack occurring in AODV. This method uses three metrics PDR (Packet Delivery Ratio), PMOR (Packet Modification Rate) and PMISR (Packet Misroute Rate), to decide the behavior of a node. The information required by the metrics is collected from all the nodes in the network. These metrics are compared to a threshold, according to which the node is considered malicious or not.

The authors in [13] propose a defense mechanism against a cooperative black hole attack that relies on the AODV routing protocol named SSP-AODV Protocol. They have incorporated two techniques: A* search algorithm and Floyd-Warshall's algorithm in the AODV routing process. And they have used the value of hop count and the estimated time as input in these two algorithms to decide the shortest secure path. A modified algorithm to improve the security and performance of the AODV protocol against the black hole attack from in [14]. In this algorithm, the authors used several new rules to identify the destructive nodes according to the node's behaviors in an Ad Hoc network and delete them from routing.

Our proposed technique differs from the techniques cited on literature review in that it focuses on forwarding only the valid route reply to the next node, even in the case of one or more black hole attacks, by sending twice the same packet reply with the difference of plus one in the sequence number to determine whether the second packet corresponds to the first.

2.1 Security Requirements of VANET

A system can be vulnerable to various system weaknesses which can be exploited by malicious element for various reasons. To make a system secure, the security requirements of a system must be addressed. There are some security requirements of the VANET system which are briefly described below. Also, figure 4 shows the kinds of possible attacks that can compromise security requirements in VANET [15].

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

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

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

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

Non-Repudiation: one of the important security requirements of VANET. Non-Repudiation ensures a sender or a receiver from denial of the transmitted data from them [16]. VANET security requirements and the possible threats to those requirements are outlined in figure 4 below.

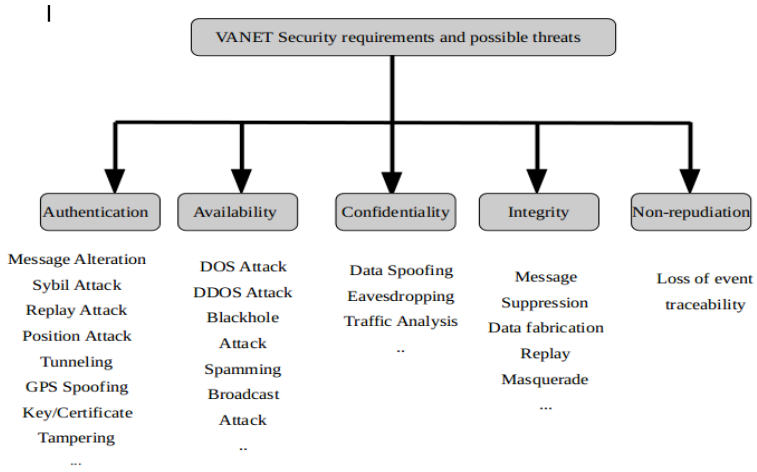

Fig.1 VANET Security Requirements and Possible Threats

2.2 AODV routing protocol

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

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

3. SECURITY ISSUES IN VANET

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

VANET still has much vulnerability which can be exploited by the attackers. Before the adoption of VANET in the real world, the different layers of VANET must be made secure. Some various threats and attacks are present in different layers of the VANET system.

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

Countermeasures

The countermeasures of network layer attacks mostly depend on the type of routing protocol used in VANET. In general, various security mechanisms such as cryptography-based algorithm, the trust-based approach can be implemented to defend against attacks on the network layer. Since this paper deals with the black hole attack on the AODV routing protocol, a filed verification based approach is adopted.

4. STATEMENT OF THE PROBLEM

Due to the nature of dynamic network topology, routing in vehicular ad-hoc network play a vital role in the performance of the networks. Understandably, most of the security threats target routing protocols – the weakest point of the vehicular ad-hoc network.

There are various studies and research in this field in an attempt to propose more secure protocols. However, there is not a complete routing protocol that can entirely secure the operation of one network in every situation.

The packets in the VANET contain highly important and confidential information and hence these packets should not be hampered or modified by malicious packets. Likewise, the drivers who update traffic information should also be subjected to liability by providing correct and timely updates.

Mobility, size of the network and geographic relevancy makes it complex to implement security in VANET.

By implementing secure AODV routing protocols and running these routing protocols in malicious environments, we hope that we will protect the black hole attack and improve the performance of these secure routing protocols.

5. PROPOSED METHOD

As mentioned before, most of the routing protocols for Ad-hoc networks were developed a long time ago without considering their security mechanism. Hence, those routing protocols are prone to various attacks. In this section, we will describe in detail our proposed solution to prevent the black hole attack that we have integrated with the AODV routing protocol.

In our approach like the standard AODV routing protocol, the destination node or intermediate node generates the RREP packet but it also generates another RREP packet. It is a kind of confirmation of the first packet with a sequence number incremented by one.

Therefore, we have two RREP messages from the destination node or an intermediate node that has the route to the destination one with the normal sequence number and the other with the normal sequence number + 1 and both have the field VERIFIED set to 0. When the intermediate node receives the RREP packet it stores the information about the packet reply then it checks our appended field VERIFIED if it is set to 0 or 1. If it is 0 that means that our packet is not yet verified or it is an invalid packet otherwise the packet is verified and valid and it must be forwarded to the next node.

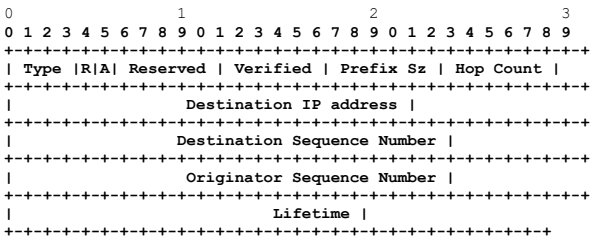

Fig.2 Format of the modified Route Reply (RREP) Message

In case of the field VERIFIED is 0 and the intermediate node receives a second route reply message it must verify if the first route reply's sequence number is the second reply's sequence number minus one; if the verification is true it sets the field VERIFIED to 1 and forward the packet.

Our approach based on the four steps detailed below:

Step 1: (Initialization Process)
Start the route discovery phase with the source node S.
Step 2: (Generation of RREPs)
The destination node or the intermediate node generates two route reply with two different destination sequence number, the second one must be incremented by one.
sendReply(seqno, // Dest Sequence Num
VERIFIED = 0,); // Appended field
sendReply(seqno+1, // Dest Sequence Num
VERIFIED = 0,); // Appended field
Step 3: (Verification of RREPs)
if (intermediate node receives RREP){
if (the first time the node receives RREP){
Store the IP address and seqno of the node;
if (RREP is valid){
Forward RREP; }
} else if (the node receives more than one RREP){
Store the IP address and seqno of the node;
if (RREP is invalid){
if (new RREP's seqno == old RREP's seqno + 1){
VERIFIED = 1; //(Mark RREP as valid)
Forward RREP;
} else {
Ignore RREP; }
} else {
Forward RREP; }
}}
Step 4: (Continue default process)
The source node sends data to the destination node from the selected route reply packet.

Also,when the intermediate node receives another route reply from the malicious node which performs a black hole attack with a very high destination sequence number. The same procedure explained will be repeated and in this case, the verification will be false, therefore, the intermediate node leaves the field VERIFIED set to 0 and ignores the packet. Our solution avoids the black hole attack and also a multiple black hole attack. In addition, the control messages from the malicious node, are not forwarded in the network.

Table 1 Fields of RREP Message

Type	Forced to 2.
R	Repair flag; used for multicast.
A	Acknowledgment required.
Reserved	Sent as 0; ignored on reception.
Verified	One bit specifies the packet Route Reply if it is valid or not as illustrated below: 0 refer to the invalid RREP 1 refer to the valid RREP
Prefix Sz	If nonzero, the 5-bit Prefix Size specifies that the indicated next hop may be used for any nodes with the same routing prefix (as defined by the Prefix Size) as the requested destination.
Hop Count	The number of hops from the Originator IP Address to the Destination IP Address. For multicast route requests this indicates the number of hops to the multicast tree member sending the RREP.
Destination IP address	The IP address of the destination for which a theroute is supplied.
Destination Sequence Number	The destination sequence number associated to the route.
Originator Sequence Number	The IP address of the node which originated the RREQ for which the route is supplied.
Lifetime	The time in milliseconds for which nodes receiving the RREP consider the route to be Valid.

6. METHODOLOGY OF EVALUATION

A. Simulation Environment

The simulations are done using NS-2 (v-2.35) networksimulator [27] to analyze the performance of our proposed solution against black hole nodes. In an area of 500x500 m, 25 nodes are randomly distributed, they execute once the standard AODV and another time the M-AODV (Modified AODV) routing protocol for comparing the two protocols under the black hole attack. For the malicious nodes are also randomly distributed. Five pairs were randomly chosen for data communication, each sending 512 bytes per second. All nodes were moved in

a Random-way point model, with random speeds ranging between 0 and 30m/s. In addition, the pause time of the nodes is 10s. The simulation parameters are summarized in table 2. Therefore, each data point represents an average of twenty runs.

B. Metrics used for Simulation

In order to evaluate the performance of our approach, we have used the following metrics:

1) Packet Delivery Ratio (PDR):It is the ratio of the total A numberof data packets received by the destination nodes and the total number of data packets generated by the source nodes. Hence, the packet delivery ratio shows the total number of data packets that reach the destination successfully. A higher packet delivery ratio shows higher protocol performance.

2) Average End-to-End Delay: It can be defined as the time elapsed between the moment of sending of a bit by the source node and the moment of its reception by the destination node. it includes all possible delays taken by the router to seek the path in the network such as buffering during route discovery latency, queuing at the interface queue, propagation, retransmission delays at the MAC and transfer times. The average end to end delay is measured in milliseconds.

3) Normalized Routing Overhead: This metric denotes the number of routing control packets generated per data packets transmitted. It is called Normalized Routing Overhead or Normalized Routing Load.

Table 2. Simulation Parameters

Parameter Value
Coverage Area 500x500 m
Number of nodes 25
Simulation time 200s
Transmission range 50m
Mobility model Random waypoint
Data Rate 0.25
Packet Size 512 Bytes
Routing Protocol AODV / S-AODV
Mobility speed 0-30 m/s
No of black hole nodes 1 and 5
Connections 5
Traffic type UDP–CBR
Pause time 10s

7. SIMULATION RESULTS AND ANALYSIS

A. Packet Delivery Ratio

The Fig. 5 and the Fig. 6 show the packet delivery ratio ofAODV, our solution and AODV under one black hole node and under-five black hole attackers when node mobility

increases. It is clear from the figures that the performance of our approach is superior over AODV under a black hole attack either for one or multiple attackers. The PDR of AODV under one attack was approximately 15%, while the PDR of Modified AODV in the presence of one attack was approximately 60%, increased by 45%. Similarly, the PDR of AODV under multiple attacks was approximately 7%, which was increased by 43% when compared to our scheme also under multiple attacks. Moreover, the PDR of the AODV routing protocol without any attacks is around 64%, which is due to congestion in the network.

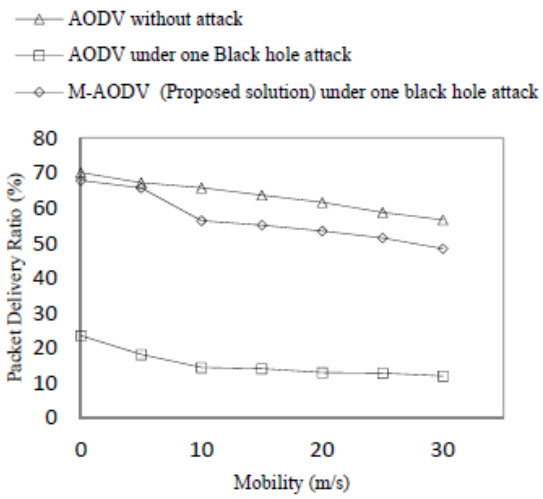

Fig.2 Packet delivery ratio vs. mobility with one attacker

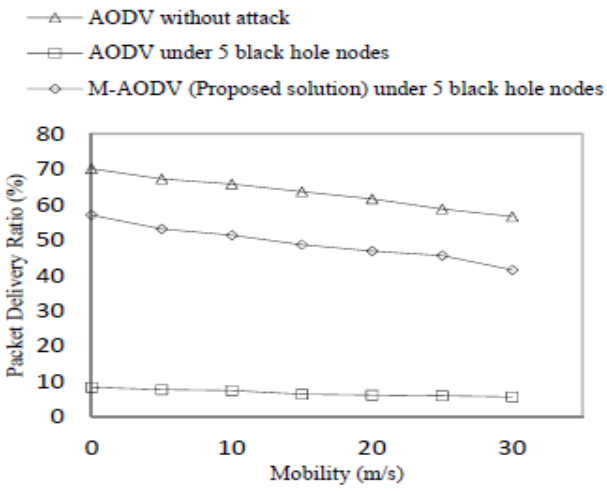

Fig.3 Packet delivery ratio vs. mobility with five attackers

B. Average End-to-End Delay

From the Fig. 7 and Fig. 8, it can be observed that, when the Modified AODV protocol is used, there is an increase in the average end-to-end delay, compared to the standard.

AODV routing protocol without attack. Also, we observe that our approach under one attack is slightly increased in the average end-to-end delay, compared to under multiple attackers. This is due to the additional waiting time in each intermediate node before sending the reply, and when there is a multiple attack our approach nee3d more time to calculate the right route reply than when one attack exists. The end to end delay in the presence of attackers in the AODV is the fewer in the two cases, either in the presence of one black hole node or in the presence of multiple attackers. This is because of the immediate reply from the malicious node, which doesn't check its routing table for the route availability.

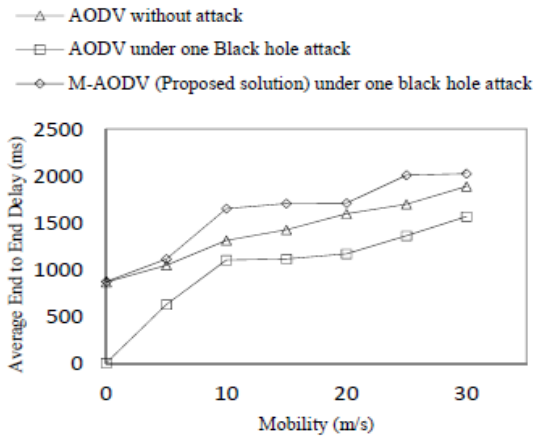

Fig. 4 Average end to end delay Vs. mobility with one attacker

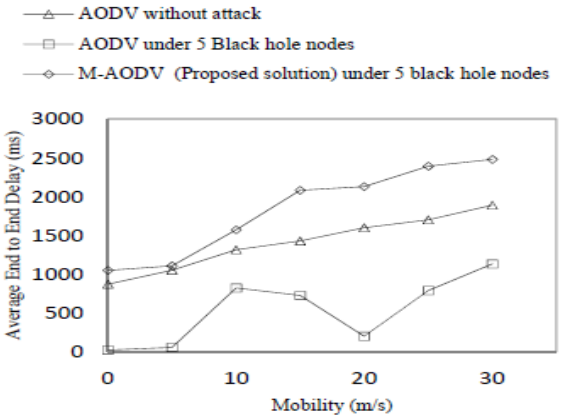

Fig.5 Average end to end delay vs. mobility with five attackers

C. Normalized Routing Overhead

The normalized routing overhead is shown in Fig. 6 and Fig. 7 while varying mobility. In our modified AODV, the routing overhead under one or multiple malicious nodes is slightly higher compared to the standard AODV because of the additional process involved to avoid the selection of malicious nodes. The normalized routing overhead for AODV under black hole attack, whether one or multiple attacks isvery high compared to the AODV without attack. This is due to the black hole nodes that send false replies to the route request packets which compromise the routing protocol then the protocol starts misbehaving and generating additional routing packets.

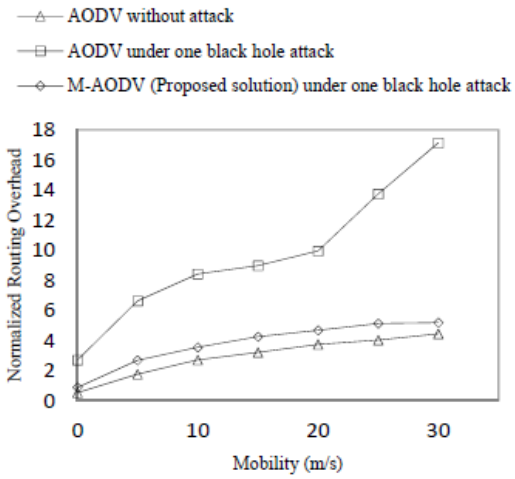

Fig.6 NRL vs. mobility with one attacker

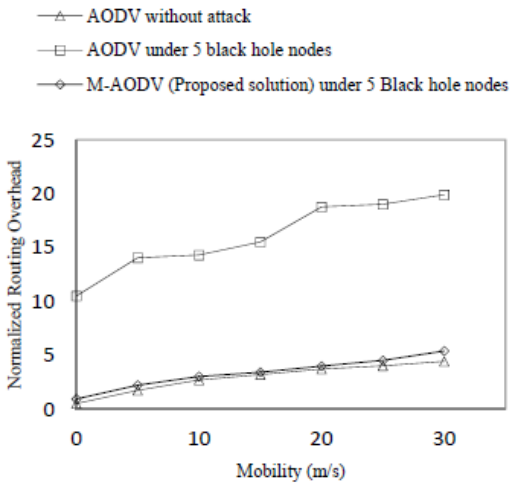

Fig.7 NRL vs. mobility with five attackers

D. Evaluation of the Number of the Dropped

Packets by theBlack Hole Attack in AODV and M-AODV We have calculated the rate of the number of packets sent, dropped and received in both cases with one black hole attack and five attackers in the standard AODV routing protocol and also in our modified AODV, as shown in Fig. 8 and Fig. 9.

In this simulation, 25 nodes are moving randomly with maximum speed at 10 m/s, 10s for pause time, the number of connections is 5 and the number of packets flowing through the network is 2849 packets. From the simulation, we definitely assert that our proposed scheme overcame the black hole attack when there is a single black hole attack and even when there are multiple attackers. For the difference between sent packets and the sum of the packets dropped and receivedpacket is due to the packets dropped in case of a collision orbuffering or other reasons.

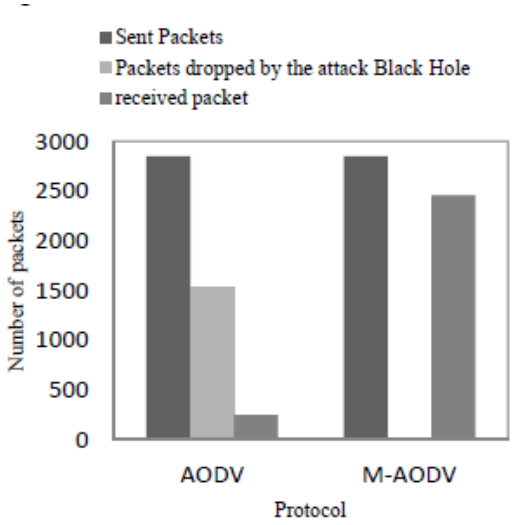

Fig.8 Number of packets flowing through the network vs. protocols with one attacker

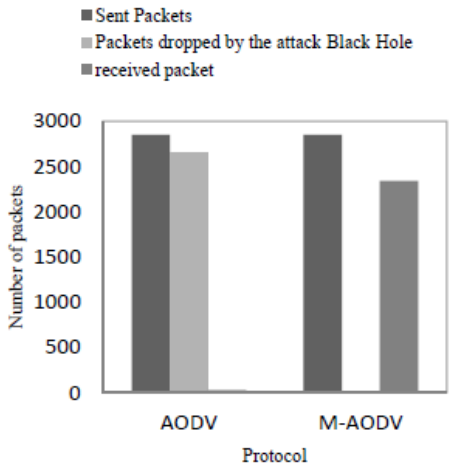

Fig.9 Number of packets flowing through the network vs. protocols with five attackers

8. CONCLUSION

Ad hoc routing protocols are prone to various attacks due to the ignorance of the security aspect during their designs. A black hole attack disrupts normal network functionality by sending bogus routing information during the route discovery phase. In this paper, we proposed a solution to avoid the black hole and the multiple black hole attackers on the AODV routing protocol in VANETs. According to the simulation results, the modified AODV gives a significant improvement in the packet delivery ratio with an acceptable average end-to-end delay and normalized routing overhead when the mobility of nodes increases. Consequently, we concluded that our proposed approach shows superior performance than the AODV in the presence of one or multiple black hole nodes.

REFERENCES

1. SalimLachdhaf, Mohamed Mazouzi, and Mohamed Abid(2017), Detection and Prevention of Black Hole Attack in VANET Using Secured AODV Routing Protocol, International Conference on Networks &Communications, Dubai, pp. 25-36
2. HeithemNacer and Mohamed Mazouzi (2016), A Scheduling Algorithm for Beacon Message in Vehicular Ad Hoc Networks. International Conference on Hybrid Intelligent Systems, Marrakech, Morocco, pp. 489-497
3. R.GaneshBabu (2016), HELIUM'S ORBIT INTERNET OF THINGS (IOT) SPACE, International Journal of Computer Science & Wireless Security, Vol.03, No.02, pp.123-124
4. Elias C. Eze, Sijing Zhang and Enjie Liu (2014), Vehicular Ad Hoc Networks (VANETs): Current State, Challenges, Potentials and Way Forward, Proceedings of the 20th International Conference on Automation & Computing, Cranfield University, Bedfordshire, UK, p. 2014
5. S.Gurmukh, P.Kumari and S.Agrawal (2015), Comparative Analysis of Various Routing Protocols in VANET, In Proceedings of 5th IEEE International Conference on Advanced Computing & Communication Technologies, Haryana, India, p. 2015
6. SabihurRehman, M. Arif Khan, Tanveer A. Zia, LihongZheng (2013), Vehicular Ad -Hoc Networks (VANETs) - An Overview and Challenges. Journal of Wireless Networking and Communications, pp. 29 - 38
7. C. Perkins, Belding-Royer, E., & Das, S (2003), Ad hoc on-demand distance vector (AODV) routing, p. 356
8. Perkins, C. E. and Bagwig, P (1994), Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers, p. 1994
9. R.GaneshBabu, and Dr.V.Amudha (2015), PERFORMANCE ANALYSIS OF DISTRIBUTED COORDINATED SPECTRUM SENSING IN COGNITIVE RADIO NETWORKS C, Middle East Journal of Scientific Research, Vol.23, No.23, pp.50-55
10. Johnson, D. B. and Maltz, D. A (1996), Dynamic source routing in ad-hoc wireless networks. In Mobile computing, Springer US pp. 153-181
11. P.Karthika and P.VidhyaSaraswathi (2017), CONTENT BASED VIDEO COPY DETECTION USING FRAME BASED FUSION TECHNIQUE, Journal of Advanced Research in Dynamical and Control Systems, Vol. 9, No. 17, pp. 885-894
12. A.Nedumaran and V.Jeyalakshmi (2015), CAERP: A CONGESTION AND ENERGY AWARE ROUTING PROTOCOL FOR MOBILE AD HOC NETWORK, Indian Journal of Science and Technology. Vol.8, No.35, pp.1-6
13. Jaisankar, N., Saravanan, R. and Swaour, K. D (2010), A novel security approach for detecting black hole attack in MANET, In Information Processing and Management .Springer Berlin Heidelberg., p, pp. 217-223
14. Patel, M. and Sharma, S (2013), Detection of malicious attack in manet a behavioral approach, In Advance Computing Conference (IACC), IEEE 3rd International, pp. 388-393
15. R.GaneshBabu, and Dr.V.Amudha (2016), CLUSTER TECHNIQUE BASED CHANNEL SENSING IN COGNITIVE RADIO NETWORKS, International Journal of Control Theory and Applications. Vol.9, No.5, pp.207-213

16. Ghathwan, K. I. and Yaakub, A. R. B (2014), An Artificial Intelligence Technique for Prevent Black Hole Attacks in MANET, Recent Advances in Soft Computing and Data Mining. Springer International Publishing, (pp. 121-131)
17. A.Nedumaran, S.AbdulKerim and TedrosSalih Abdu (2017), ADVANCED LINK STATE ROUTING PROTOCOL APPROACH FOR MOBILE AD-HOC NETWORKS, International Journal for Scientific Research and Development. Vol. 5, No. 3, pp.516-519
18. Shahabi, S., Ghazvini, M. and Bakhtiarian, M (2015), A modified algorithm to improve the security and performance of the AODV protocol against black hole attack, Wireless Networks, p. 2015
19. Zhou, Y., Wu, D. and Nettles, S (2004), Analyzing and Preventing MAC-Layer Denial of Service Attacks for Stock 802.11 Systems, p. 2004
20. P.Karthika and P.VidhyaSaraswathi (2018), DIGITAL VIDEO COPY DETECTION USING STEGANOGRAPHY FRAME BASED FUSION TECHNIQUES, The International Conference on ISMAC in Computational Vision and Bio-Engineering, Lecture Notes in Computational Vision and Biomechanics, vol. 30. Springer,Cham
21. Woungang, I., Dhurandher, S. K., Peddi, R. D. and Traore, I (2013), Mitigating collaborative black hole attacks on DSR-Based mobile ad hoc networks, In Foundations and Practice of Security, pp. 308-323
22. Perkins, C., Belding-Royer, E. and Das, S (2003), Ad hoc On-Demand Distance Vector (AODV) Routing, p. 2003
23. R.GaneshBabu and Dr.V.Amudha (2014), SPECTRUM SENSING TECHNIQUES IN COGNITIVE RADIO NETWORKS: A SURVEY, International Journal of Scientific and Engineering Research. Vol.5, No.4, pp.23-32
24. Network Simulator- NS-2 (2019), Available online: https://www.isi.edu/nsnam/ns/ (accessed on 5 May 2019; no. May, p. 2019, 2019
25. Yousefi, S., Mousavi, M. and Fathy, M (2006), Vehicular Ad hoc Networks (VANETs): challenges and perspectives, p. 2006
26. Li, M. Security in VANETs. [online] Cse.wustl.edu.pdf
27. Varshney, T (2019), Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network, IEEE Conference Publication, p. 2019
28. P.Karthika and P.VidhyaSaraswathi(2017), A SURVEY OF CONTENT BASED VIDEO COPY DETECTION USING BIG DATA, International Journal of Scientific Research in Science and Technology, Vol. 3, No.5, pp. 114-118
29. Thachil, F. and Shet, K (2019), A Trust-Based Approach for AODV Protocol to Mitigate Black Hole Attack in MANET, IEEE Conference Publication, p. 2019
30. R.GaneshBabu, and Dr.V.Amudha (2015), ANALYSIS OF DISTRIBUTED COORDINATED SPECTRUM SENSING IN COGNITIVE RADIO NETWORKS, International Journal of Applied Engineering Research. Vol.10, No.6, pp.5547-5552
31. J. W. Cresswell (2002), Research Design: Qualitative, Quantitative and Mixed Methods Approaches, 2nd. Ed. California: Sage Publications, p.2002
32. Rahul Krishnan, R.GaneshBabu, S.Kaviya, N.Pragadeesh Kumar, C.Rahul, and S.Santhana Raman (2017), SOFTWARE DEFINED RADIO (SDR) FOUNDATIONS, TECHNOLOGY TRADEOFFS: A SURVEY, Proceedings of IEEE International Conference on Power, Control, Signals & Instrumentation Engineering (ICPCSI' 17) with ISBN.No-978-1-5386-0814-2, Saveetha Engineering College, Chennai, India, pp.2677-2682
33. Nadeem, A. and Howarth, M. (2019), A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks. IEEE Journals & Magazine, p. 2019
34. TegegnAyalewHailu and A.Nedumaran (2019), A SURVEY ON PROVISIONING OF QUALITY OF SERVICE (QOS) IN MANET, International Journal of Research and Advanced Development, Vol. 3, No. 2, pp.34-40
35. Jalil, K., Ahmad, Z. and AbManan, J (2019), ERDA: Enhanced Route Discovery Mechanism for AODV Routing Protocol against Black Hole Attacks, p. 2019

How to cite this articles :
WubishetGirmaMekonnen, Nedumaran Arappali, "Secured AODV Routing Protocol to Improve Security in VANET", International Journal of Intelligent Computing and Technology (IJICT), Vol.3, Iss.2, pp.01-15 , 2020