A distributed trust mechanism for malicious behaviors in VANETs

Ali Kamil Ahmed[1], Mohanad Najm Abdulwahed[2], Behnam Farzaneh[3]
[1,2]University of Technology-Iraq, Department of Materials Engineering, Iraq
[3]Isfahan University of Technology, Department of Electrical and Computer Engineering, Iran

Article Info

Article history:

Received Jan 22, 2020
Revised Mar 24, 2020
Accepted Apr 8, 2020

Keywords:

Detection and prevention
Gray-hole attack
TOPSIS method
VANET
Vulnerability

ABSTRACT

Vehicular Ad-hoc Networks (VANETs) are one of the most important types of networks which are widely used in recent years. Along with all the benefits of Quality of Service (QoS) improvements, vulnerability analysis for this type of networks is an important issue. For instance, a Gray-hole attack decreases network performance. We proposed a novel solution to help to secure these networks against this vulnerability. The proposed method can detect and prevent the Gray-hole attack. Anywhere in the network, each node (vehicle) can distinguish between the Gray-hole attack and the failed link. Some topology related information helps us to detect attacks more accurately. Also, the proposed method uses the most reliable path in terms of link failure when there is no malicious node. In this paper, we used the TOPSIS method for choosing the most trusted node for routing intelligently. We validated our proposal using a simulation model in the NS-2 simulator. Simulation results show that the proposed method can prevent Gray-hole attack efficiently with low overhead.

Corresponding Author:

Ali Kamil Ahmed,
Department of Materials Engineering,
University of Technology-Iraq,
Al-Wehda neighborhood, Baghdad, Iraq.
Email: 130070@uotechnology.edu.iq

1. INTRODUCTION

Vehicular Ad-hoc Networks (VANETs) considered as one of the main components of Intelligent Transportation Systems (ITS). The researchers and automotive industries are interested to it in the last few decades. These networks use for safety, entertainment, and service by the users [1]. VANET consider as a subset of moving ad-hoc networks, where vehicles represent the moving nodes, and also they are the same as moving ad-hoc networks in self-organizing, self-management, and low bandwidth and transmission conditions. Due to high Bit Error Rate (BER), shading, fading and interference phenomenon as well as dynamic topology in VANET, they have failed connections, and for the fast-moving vehicles, the probability of packet loss is very high [2, 3]. Since the lack of the central linking coordinator, there are some challenges in VANET. The expansion of wireless communication networks in VANET needs to solve some inherent issues such as economic and technical applications [4]. Some of the challenges in VANET, for achieving effective vehicle communications, are as follows [5, 6]: Multicast messages, Bandwidth limited, Routing protocols, Power control and management, privacy and security. Security plays an important role in VANET. Also, the lack of a central structure for VANET is one of the challenges facing these types of networks [7]. Also besides security and privacy, practical methods for attack detection and prevention are a serious issue in the practical implementation of VANETs [8, 9]. Figure 1 shows the secure routing architecture in VANETs. There are various types of attacks on VANET listed as follows:

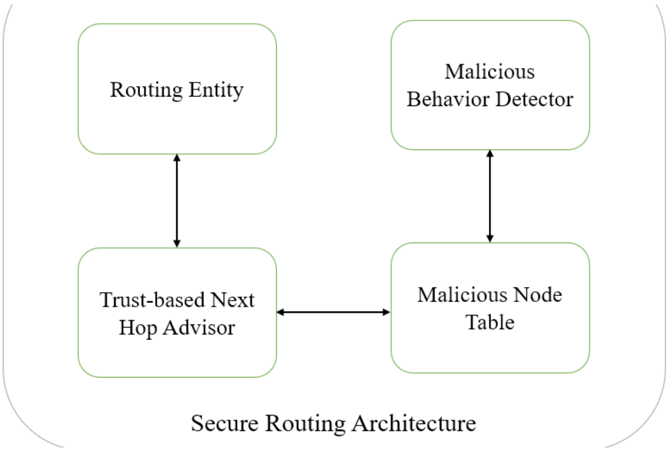

Routing Entity
Malicious Behavior Detector
Trust-based Next Hop Advisor
Malicious Node Table
Secure Routing Architecture

Figure 1. The security routing architecture in VANETs

A. Attacks on Availability

In these types of attacks, the attacker tries to temporarily interrupt or suspend the services. This attack targets network resources or vehicles to make them unavailable [10]. Denial of Service attack (DOS) is one of the famous attacks. By these attacks, valid users cannot access the network. The black-hole attack is in this category. In [11] authors used beacon for DOS attack detection and prevention. There is another attack called Distributed Denial of Service attack (DDOS). It is a DOS attack, where distributed attackers cooperate to target network availability [12].

B. Attacks on Confidentiality

As understood from the name of this attack, the attacker tries to access some private information of the victim. This attack can be implied to the wireless link because of the natural feature of it [13].

C. Black-hole Attack

In the Black-hole attack, the attacker appears itself as a cooperative node to provide the shortest path in the network, so this virtual node doesn't allow data packets to reach the destination. The attacker node which causes a Black-hole in the network called a malicious node. If a malicious node does not behave maliciously all the time, the attack called a Gray-hole attack, which is the general form of the Black-hole attack. Due to the fact that sequence number plays an important role in Ad hoc On-Demand Distance Vector (AODV) routing protocol, a malicious node tries to manipulate this parameter. Malicious node makes false RREP to the source node with a high sequence number and absorbs all the packets [13].

There are two types of Black-hole attack. The first is a single Black-hole attack or a non-cooperative and the other one is a cooperative Black-hole attack. In the first one, the malicious node tries to show itself the best node and receives all the network traffic, then it drops all the packets, which reduces network performance severely. In the cooperative Black-hole attack, there are many malicious nodes that work together to influence network performance [14]. Intrusion Detection and Prevention System can be used for monitoring network operations and detect intruders [15, 16].

In this paper, we assume only one malicious node exists but it is not malicious at all the time. In other words, we concentrate on a single Gray-hole attack. In [17], authors are introduced another attack called Degrading Quality of Service (DQoS). This attack is similar to the Gray-hole attack. The attacker takes place between Road Side Unit (RSU) and vehicles to prevent data reception by vehicles. Therefore, RSU resources drop and QoS decreases. In this paper, the authors are concentrated on the authentication process to mitigate the attack.

The rest of the paper is as follows: Section 2 is the research background for providing an overview of other solutions in the literature. Section 3 presents the motivation of this study. Section 4 outlines the proposed method for overcoming the Gray-hole attack issue. This section has two main parts. The first part illustrates the attack detection mechanism and the second part describes how the proposed method prevents the Gray-hole attack. In Section 5, the proposed method is evaluated. Finally, in Section 6, conclusions are described.

2. RESEARCH BACKGROUND

In audit-based methods, some nodes recognize the Black-hole attack by monitoring all nodes in the network. Watchdog methods for auditing nodes in the Mobile Ad-hoc Networks (MANETs) are proposed in [18]. Where, the neighbors of each node find the sender of the false information and the Black-holes attacked, by observing the received and sent data by the node. In this method, the performance reduces with increasing the mobility speed and noise of the node in the network, which made it unsuitable for VANET networks. In [19], more precise methods were offered for improving the detection of a Black-hole attack. These methods based on the cooperation of neighboring nodes using the Bayesian Watchdog method. Although the cooperation of the neighboring nodes have improved the recognizing of the Black-hole attack, it still has the same problem as the previous method.

In [20], by monitoring the network statistics, the target and source nodes detect and prevent Black-hole attacks. Although this method can detect a Black-hole attack after routing, it is not useful during routing. This kind of attack during the routing password is used. In [21], a method defined as SAODV is used to contrast a Black-hole attack of confidentiality and validation. This method is good to prevent the target node impersonation by destructive nodes, but it does not provide a solution to disposal false packets. The method based on the authentication is used in [22] and known as the TWO-ACK method. Although this method prevents Black-hole attacks, it isn't useful in VANET networks because of the complexity and overloading.

In [23], a reputation-based approach is used to overcome Gray-hole issues in mobile ad-hoc networks. This manner uses a trust model in the AODV routing protocol. The reliability of nodes is estimated during route discovery. In [24], the AODV routing protocol was developed to reduce the accessing of the path by a Black-hole node. The protocol is known as the RREP'2 protocol. In this protocol, the source node throws out the first or the first two preceding of received RREP. Continually, it selects each received RREP packet. Because the RREP created by the Black-hole node is the first or second received RREP to the source node. This protocol can be very useful when the Black-hole node is located near the source node. In [25], a proposed modified AODV routing protocol called PCBHA is introduced to prevent Black-hole attacks. In [26], a new solution was proposed to contrast Black-hole attacks in VANET networks called DPRAODV (Detection, Prevention, and Reactive AODV) for preventing co-operative Black-hole attack in MANET. This method is the same as Tamilselvan and Sankaranarayanan. But in this method, they provided a mechanism for blocking the Black-hole node in a dynamic mechanism process.

3. MOTIVATION

Among the security challenges in VANETs, malicious nodes (vehicles) are major threats for the network and its participated vehicles. The main problem is when an authenticated vehicle shows malicious behavior on the network. Therefore, vehicle communications are not secure based on the messages received by such vehicles. Therefore, designing a system to identify such abuses is essential for VANETs. Many mechanisms have been proposed so far to detect and prevent malicious behaviors in VANETs. Each method has its disadvantages, although effective in proceeding the detection and prevention of malicious behaviors. If the vehicle wants to judge whether a message is an authentic or not, it must first gather enough information from herself and others and then decides whether to validate the message. In a proper mechanism, the nodes in addition to detecting the malicious node, inform the other nodes about the presence of the malicious node. Then, how to route and select the next node should be such that, as far as possible, the selection of the malicious node is avoided. In the proposed method, besides avoidance of the selection of malicious nodes, an attempt is made to select a more stable link. As well as, malicious nodes should be given the opportunity again to participate in routing, because they may have been mistaken as malicious. The idea behind this paper is to present a trust-based distribution mechanism for detecting and preventing malicious behaviors in the VANETs. For this purpose, we used one of the popular Multi-Criteria Decision Making (MCDM) methods called TOPSIS to select the most trusted path.

4. PROPOSED METHOD

Our proposed method has two parts. The first part is responsible for detecting the attack and the second part is responsible for preventing the attack. We used nodes location and relative speed for attack detection. We distinguished between link failure and malicious behavior of nodes. Also, a historical behavior-based mechanism is designed to prevent the attack by removing malicious nodes from the active route.

4.1. Detection of Gray-hole Attack

As we know in AODV routing protocol, periodic Hello messages exchanged among vehicles to detect neighbors. We can use these messages to notify the vehicles about their neighbor's location and calculate relative speed. So, each node puts its speed and its (x, y) position in hello message as new fields of AODV hello message. The neighbor table which maintains neighbor information must add relative speed and distance as new information of the neighbor. The distance of the i_{th} node can be calculated as in (1):

$$d_i = \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2} \tag{1}$$

Where x_i and y_i is the i_{th} node position. To calculate relative speed, at least two hello messages are needed for detecting direction. After receiving the second hello message, the directed speed vector of the neighbor can be calculated. Also, each node can calculate its own speed vector. So, the relative speed can be calculated as in (2):

$$v_{ij} = \begin{cases} \sqrt{v_i^2 + v_j^2 - 2v_i v_j cos\theta} & \theta \neq 0 \vee 180 \\ v_i - v_j \theta = 0 \\ v_i + v_j \theta = 180 \end{cases} \tag{2}$$

where v_i is the speed of the i_{th} vehicle, v_j is the speed of j_{th} vehicle, θ is the angle between i_{th} and j_{th} vehicle motion vectors.

According to the transmission range of each node, the probability of link failure instead of malicious behavior increases with the increment of the node's distances. If the absolute value of relative speed between two nodes increases, the probability of the link failure will increase, and for the small values of relative speed, if a link failure occurs, the probability of malicious behavior of node or Gray-hole attack will increase. If the data link layer detects a link failure, it may occur a Gray-hole attack. So, we need some proper mechanisms to distinguish between real link failure and Gray-hole attack. At this point, we define D_{th} and V_{th} thresholds for attack detection. The D_{th} parameter shows the threshold distance which lower distances are considered as the attack in the link failure. In the same way, V_{th} shows a relative speed threshold in which higher relative speeds are considered as the attack in link failure.

If the Gray-hole attack is detected instead of the link failure, at first, the corresponding node considered as a malicious node. Then ATT message will be generated. This message carries the malicious node ID, to notify the source node about the attacker node ID. The ATT message goes through the reverse route to reach the source node. Each middle node in reverse route, after receiving the ATT message, puts this node ID in a table called attackers table and forwards it to the next hop. Attacker's table plays an important role in the next attacks from attackers. This table holds the last attack time and the number of attacks per attacker node. Other nodes that are not participating in the active route, they do not comprehend attack occurrence. So, the attacker node ID is added to the conventional RREQ message. As we know RREQ message spreads over the network by the source node. Other nodes will be aware of attacker ID and will update their attacker table.

4.2. Prevention of Gray-hole Attack

The AODV routing protocol uses the shortest path between the source and target without attending to anything more. The proposed method adds a property of attack awareness to the AODV routing protocol. There are four criteria in the proposed method to avoid participation in the malicious nodes in the active route during the route discovery. These criteria are distance, relative speed, number of malicious behaviors in the past and spent time from the latest attack. As seen in the previous, the distance and the relative speed are accessible in the neighbor table, and the number of attacks and the spent time from the latest attack is accessible in the attacker's table. In AODV routing protocol the source node for starting route discovery broadcasts the RREQ message. In the proposed method, if the source node has been received the ATT message, it puts the malicious node address on a modified RREQ message. The key point of the proposed method is the selection of the most trusted nodes instead of all nodes among the neighbors to send a modified RREQ message. The selection of the most trusted nodes is done by the TOPSIS method [27]. This method is one of the most popular MCDM methods. Figure 2 shows the flowchart description of the proposed method.

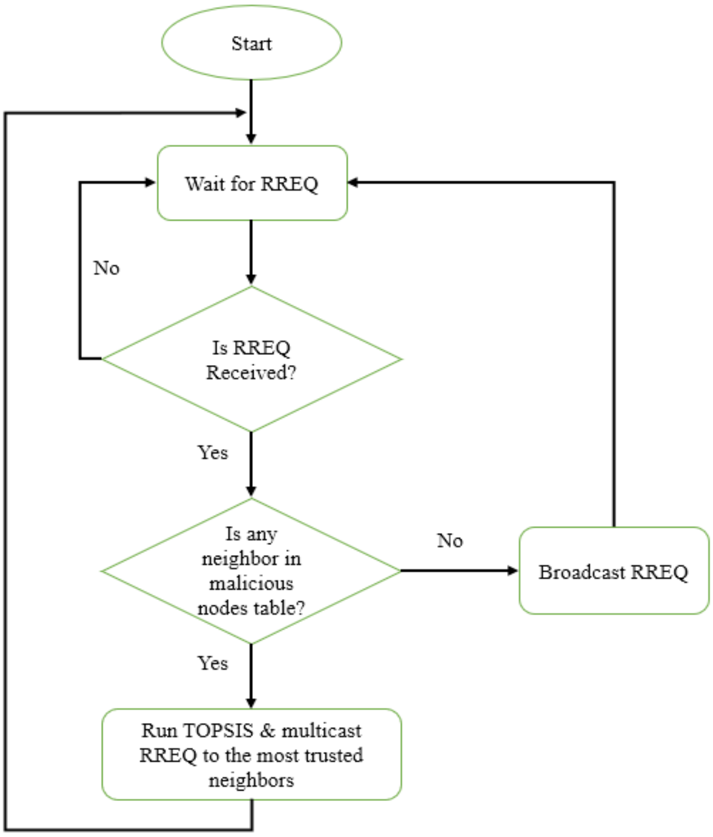

Start
Wait for RREQ
No
Is RREQ Received?
Yes
Is any neighbor in malicious nodes table?
No
Broadcast RREQ
Yes
Run TOPSIS & multicast RREQ to the most trusted neighbors

Figure 2. The flowchart description of the proposed method

4.3. TOPSIS method

In recent years, MCDM methods are widely used in network topics [28]. The TOPSIS method as a well-known MCDM introduced for the first time in 1981 [27]. In this method, each option called alternative is considered as a point in space. Then the Euclidean distance of each point is calculated from the two important points which are called the positive ideal answer (A^+) and the negative ideal answer (A^-). In the next step, points are ranked according to their distance from the positive ideal answer and the negative ideal answer.

This method gets the decision matrix as input. This matrix contains M alternatives and N criteria. The numerical value of the j_{th} criterion for the i_{th} alternative shown by X_{ij}. Initially, the value of each criterion must be checked to find their profits or losses nature. It is obvious that qualitative criteria (by scale approaches) must be changed to quantitative measures. Also, this method has another input that determines the importance of each criterion to another. It is called the decision-maker weights. Before sending each RREQ, this method will run in six steps to find the trusted neighbors.

Step 1: The vector method is used to normalize the decision matrix. The vector normalizing as in (3):

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum x_{ij}{}^2}} \tag{3}$$

The normalized matrix as in (4):

$$R_{ij} = \begin{bmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{m1} & \cdots & r_{mn} \end{bmatrix} \tag{4}$$

This is done to exclude the dimension in the problem, as each criterion may have a specific unit of measurement.

Step 2: Multiplying the weight of each criterion by the column corresponding to that criterion in the normalized matrix to obtain the matrix V, as shown in (5):

$$v_{ij} = w_j r_{ij} \tag{5}$$

Assume that $W=(w_1,w_2,\dots,w_j,\dots w_n)$ is the weight matrix for the desired criteria, multiplying the first column by w_1, and the second column by w_2, and thus multiplying the n_{th} column by w_n, as shown in (6):

$$V = \begin{bmatrix} v_{11} & \cdots & v_{1n} \\ \vdots & \ddots & \vdots \\ v_{m1} & \cdots & v_{mn} \end{bmatrix} \tag{6}$$

Step 3: Defining positive ideal options A^+ and negative A^-, as shown in (7) and (8):

$$A^{+\{(max v_{ij} \vee j \in J),(max v_{ij} \vee j \in J')\vee i=1,2,3,\dots,m\}=\{v_1^{+,,v_2^{+,,\dots,v_n^{+\}}}}} \tag{7}$$

$$A^{-\{(min v_{ij} \vee j \in J),(min v_{ij} \vee j \in J')\vee i=1,2,3,\dots,m\}=\{v_1^{-,,v_2^{-,\dots,v_n^{-\}}}}} \tag{8}$$

where J is the criteria of profit and J' is the criteria of cost.

Step 4: The geometric distance of each alternative to A^+ and A^- must be obtained. By n-dimensional Euclidean distance, the distance between each positive and negative ideal option is calculated. Assume S_i^+ is the option of i_{th} distance for A^+ and S_i^- for A^- as shown in (9) and (10):

$$S_i^{-\sqrt{\sum_{j=1}^{n}}} \tag{9}$$

$$S_i^{+\sqrt{\sum_{j=1}^{n}}}, i = 1,2,\dots,m \tag{10}$$

Step 5: For each option i, we calculate Ci as in (11):

$$C_i = \frac{S_i^-}{S_i^{\mp S_i^{+0<C_i<1}}} \tag{11}$$

As can be seen, this index represents relative distance weights between the i_{th} alternative and the negative ideal. Therefore, if the amount of C_i is more for each option, the negative ideal distance will be more and it will has a higher rate. At the best state, A_i is located on A^+ and $C_i = 0$, and in the worst case, A_i is located on A^- and $C_i = 1$.

Step 6: We compare the obtained amounts from step 5. Whenever the amounts are larger that means better.

5. SIMULATION RESULTS

The NS2.35 [29] simulator is used to evaluate and implement the proposed method. The NS simulator is a comprehensive simulation software for communication and computer networks. This simulator supports various built-in network protocols. The simulator of the real network simulator project launched in 1989 at the University of California (Berkeley). This project has been completed over the last recent years. The NS2 simulator is one of the most powerful simulators which can simulate a wide range of protocols and networks. In NS2 simulator, C++ language and Object Tool command Language (OTcL) are used as core development and commands interpreter at the same time. C++ is used to process input packets and implement protocols because of its high speed, while the OTcL language is used to simulate the topology and the structure of the network. The NS2 simulator can be considered as OTcL manuscript interpreter that consists of a library of objects and network components, network building libraries, and simulator events scheduler. It should be noted that object-orientation and some new features added to Tcl to construct OTcL language, which has been designed and implemented at MIT University.

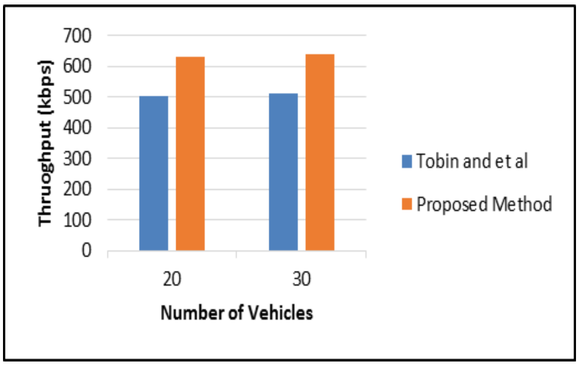
In the simulation, a random selection of the source and target vehicles was used. Also, vehicles randomly moved. During the simulation, the source and destination vehicles do not change, and traffic lights are not included at crossings. Other details of simulations can be seen in the Table 1.

Table 1. Parameters of simulation

Parameters	Amount
Simulation Time	100 seconds
Simulation Range	500 * 500
Traffic Model	CBR
Packet Size	512 bytes
Movements Producer	SUMO
Vehicles Number	20 and 30
Vehicle Speed	0-30 m / s
Number of Malicious Nodes	5
MAC / PHY	IEEE 802.11 p

Figure 3 shows the throughput of the proposed method in comparison to the Tobin et al method. According to this Figure, the proposed method could increase the throughput well because two of the parameters examined during the routing had been the distance of neighbor and relative speed. According to the TOPSIS method, next-hop candidates are chosen from near and low relative speed neighbors. This causes selection a more reliable path. So, the usage of these parameters in the next-hop selection procedure increases route stability and throughput. Also, throughput increases under attack condition, since malicious node prevention based on the last attack time and the number of attacks. The TOPSIS multi-criteria decision making plays an important role in this enhancement. In the proposed method, if a node marked as a malicious node mistakenly, it has another chance to participate in the active route. This causes throughput enhancement in sparse networks.

Figure 4 compares the proposed method with the Tobin et al method in means of routing overhead. Tobin et al method [20] is based on the query from all intermediate nodes in the active route which implies a lot of overhead in the network. Whereas the proposed method has impressive overhead. Notably, sending RREQ messages to the most trusted neighbors instead of broadcasting it to all neighbors causes an overhead reduction in the network. Also, the proposed method prevents receiving the RREQ message by the malicious node. So, this node cannot broadcast the RREQ message and network overhead decrease by the means of decreasing the number of nodes that broadcast RREQ.



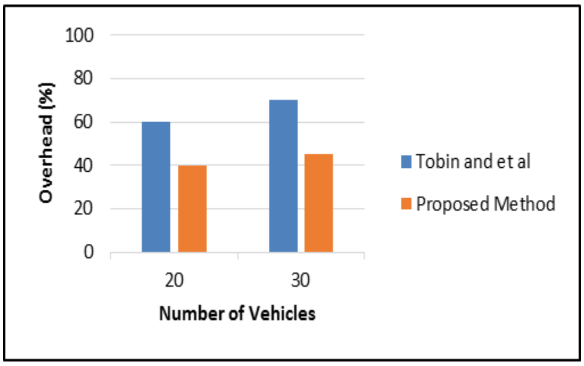


Figure 3. Throughput of the proposed method in comparison to Tobin et al method

Figure 4. Comparison the proposed method with Tobin et al method in means of routing overhead

Figure 5 shows the packet delivery ratio in the proposed method and Tobin et al method. Due to packet delivery ratio reduction in Gray-hole attack conditions, our proposed method uses two manners to overcome this issue. The first one is avoiding to add suspicious nodes in the active route and the second one is the selection of the most reliable neighbors in the case of neighbors are not suspicious (not malicious node). The proposed method is a link quality-aware routing protocol beside a trust-based routing mechanism. The integration of these mechanisms enhances the route stability in normal and under attack conditions. So, both insecure and non-stable routes will be deleted in the routing procedure. As a result, the packet delivery ratio will be increased.

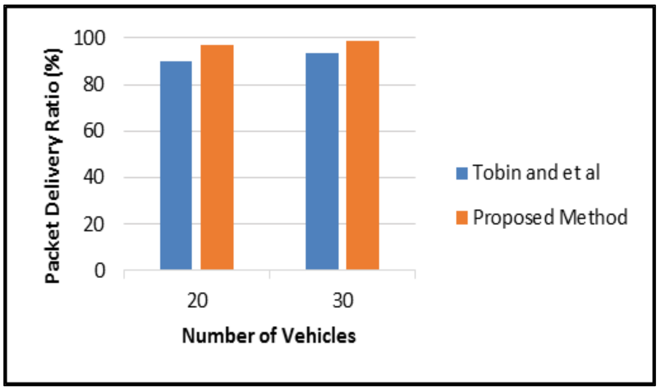


Figure 5. Comparison packet delivery ratio in the proposed method and Tobin et al method

6. CONCLUSION

One of the main goals in VANETs is to send secure messages to increase the security of vehicles along the path. Due to the high sensitivity of the security message, and the necessity of authenticity of the message content, many efforts have been made to detect and prevent malicious behaviors in VANETs. This paper introduced a novel method for Gray-hole attack detection and prevention. In this method, a new idea was used so each node can distinguish between the Gray-hole attack and the failed link. Some topology related information i.e. related speed and location information, helped us to detect attacks more accurately. At the prevention phase, the most trusted path was selected and malicious nodes do not participate in the active route. Well-known TOPSIS multi-criteria decision-maker method, helped us to select the most trusted path. Results of simulation explain that the proposed method increases throughput and packet delivery ratio under attack conditions with low overhead.

REFERENCES

[1] J. T. Isaac, et al., “Security attacks and solutions for vehicular ad hoc networks,” *IET communications*, vol. 4, no. 7, pp. 894-903, 2010.

[2] J. Liu, et al., “A survey on position-based routing for vehicular ad hoc networks,” *Telecommunication Systems*, vol. 62, no. 1, pp. 15-30, 2016.

[3] S. A. A. Shah, et al., “Adaptive beaconing approaches for vehicular ad hoc networks: A survey,” *IEEE Systems Journal*, vol. 12, no. 2, pp. 1263-1277, 2018.

[4] G. Li, et al., “Adaptive quality-of-service-based routing for vehicular ad hoc networks with ant colony optimization,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3249-3264, 2016.

[5] C. Campolo, et al., “Vehicular Ad hoc Networks,” Springer International Publishing, pp. 1-543, 2015.

[6] C. H. Goya, et al., “Cooperation requirements for packet forwarding in vehicular ad-hoc networks (VANETs),” in *Proceedings of the International Conference on Computer Systems and Technologies and Workshop for PhD Students in Computing*, pp. 1-6, 2009.

[7] S. S. Manvi and S. Tangade, “A survey on authentication schemes in vanets for secured communication,” *Vehicular Communications*, vol. 9, pp. 19-30, 2017.

[8] J. Weng, et al., “Benbi: Scalable and dynamic access control on the northbound interface of sdn-based vanet,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 1, pp. 822-831, 2018.

[9] C. Huang, et al., “Vehicular fog computing: Architecture, use case, and security and forensic challenges,” *IEEE Communications Magazine*, vol. 55, no. 11, pp. 105-111, 2017.

[10] V. Bibhu, et al., “Performance analysis of black hole attack in VANET,” *International Journal of Computer Network and Information Security*, vol. 4, no. 11, p. 47-54, 2012.

[11] K. Verma, et al., “Prevention of DoS attacks in VANET,” *Wireless personal communications*, vol. 73, no. 1, pp. 95-126, 2013.

[12] P. Saravanan and T. Sethukarasi, “Optimal Hop Selection Based Novel Trust Based DDoS Attack Removal Framework for Reliable and Secured Transmission of Data in VANETs,” *Wireless Personal Communications*, pp. 1-29, 2019.

[13] A. Rawat, et al., “VANET: Security attacks and its possible solutions,” *Journal of Information and Operations Management*, vol. 3, no. 1, pp. 301-304, 2012.

[14] A. Sharma and S. Jain, “A Behavioral Study of AODV with and without black hole attack in MANET,” *International Journal of Modern Engineering Research*, vol. 1, no. 2, pp. 391-395, 2011.

[15] B. Farzaneh, et al., “An Anomaly-Based IDS for Detecting Attacks in RPL-Based Internet of Things,” in *2019 5th International Conference on Web Research (ICWR)*, pp. 61-66, 2019.

[16] B. Farzaneh, et al., “A New Method for Intrusion Detection on RPL Routing Protocol Using Fuzzy Logic,” in *IEEE 6th International Conference on Web Research (ICWR)*, 2020. [unpublished]

[17] A. Yang, et al., “DeQoS Attack: Degrading Quality of Service in VANETs and its Mitigation,” in *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 4834-4845, 2019.

[18] J. Hortelano, et al., “Watchdog intrusion detection systems: Are they feasible in manets,” *XXI Jornadas de Paralelismo*, pp. 7-10, 2010.

[19] M. D. Serrat-Olmos, et al., “Accurate detection of black holes in MANETs using collaborative bayesian watchdogs,” in *2012 IFIP Wireless Days*, pp. 1-6, 2012.

[20] J. Tobin, et al., “An approach to mitigate black hole attacks on vehicular wireless networks,” in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, pp. 1-7, 2017.

[21] M. G. Zapata, “Secure ad hoc on-demand distance vector routing,” *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 6, no. 3, pp. 106-107, 2002.

[22] D. Dave and P. Dave, “An effective Black hole attack detection mechanism using Permutation Based Acknowledgement in MANET,” in *IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 1690-1696, 2014.

[23] N. Arya, et al., “Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm,” in *2015 International Conference on Computer, Communication and Control (IC4)*, pp. 1-5, 2015.

[24] A. Chaturvedi and S. Sharma, “A new technique for preventing black hole attack in mobile ad-hoc networks,” *International Journal of Advances in Computer Science and Technology*, vol. 3, no. 10, pp. 446-451, 2014.

[25] T. Latha and V. Sankaranarayanan, “Prevention of co-operative black hole attack in MANET,” *Journal of Networks*, vol. 3, no. 5, pp. 13-20, 2008.

[26] P. N. Raj and P. B. Swadas, “Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet,” *International Journal of Computer Science Issues (IJSCI)*, vol. 2, pp. 54-59, 2009.

[27] H. S. Shih, et al., “An extension of TOPSIS for group decision making,” *Mathematical and computer modelling*, vol. 45, no. 7-8, pp. 801-813, 2007.

[28] B. Farzaneh, et al., “MC-RPL: A New Routing Approach based on Multi-Criteria RPL for the Internet of Things,” *2019 9th International Conference on Computer and Knowledge Engineering (ICCKE)*, pp. 420-425, 2019.

[29] T. Issariyakul and E. Hossain, “Introduction to network simulator 2 (NS2),” Springer, pp. 21-40, 2012.