SRTTU

Journal of Electrical and Computer Engineering Innovations
(JECEI)
Journal homepage: http://www.jecei.sru.ac.ir

JECEI

PAPER TYPE (Research paper)

A New Framework for Secure Routing in VANET

S. Goli-Bidgoli*, M. Mousa SofarAli

Department of Computer Engineering, Faculty of Electrical and Computer Engineering, University of Kashan, Kashan, Iran.

Article Info

Article History:
Received 20 August 2017
Revised 03 January 2018
Accepted 06 April 2018

Keywords:
Routing
Reliability
Trust
Security
VANET

*Corresponding Author's Email Address:
salmangoli@gmail.com

Extended Abstract

Background and Objectives: Vehicular Ad-Hoc Networks can enhance road safety and enable drivers to avoid different threats. Safety applications, mobile commerce, and other information services are among different available services that are affected by dynamic topology, vehicle's speed and node misbehaving. Dynamic topology makes the route unstable and unreliable. So, improving the throughput and performance of VANET through reliable and stable routes with low overhead are among the important goals in this context.

Methods: Verifying all issues related to the reliable routing, different effective internal, external and environmental factors on route reliability are led to a new security framework in this paper. Black-hole attack and its effects, as the most well-known attack in wireless networks, along with presenting a secure routing protocol are other achievements of this paper. The proposed protocol uses a trust management system to detect and neutralize this type of attack.

Results: Simulation results show that the presented trust-based framework can increase the reliability of the networks by decreasing the effect of the malicious nodes in the routing process.

Conclusion: Our simulation results show that the proposed protocol can overcome the effects of black-hole attackers and it can increase throughput by 93% and packet received rate by 94.14% compared to the original AODV. Investigating the effect of the other attacks, simulating in an urban area with repetitive communications and considering the RSU in verifying the trustworthiness of entities are suggested for our future works.

Introduction

The Vehicular Ad-Hoc Network (VANET) is a subset of Mobile Ad-hoc Networks (MANETs) which plays an important role in improving the safety of the network. A vehicle moves and communicates with others in a range of 100 to 300 meters [1]. Vehicle-to-vehicle (V2V) and vehicle-to-Infrastructure (V2I) are two types of these communications. Exchanging safety messages can lead to traffic decrease and reliability increase [2]. So, the main aim of VANET is to use safety and non-safety messages to make driving safer and reduce traffic and accidents. Several different applications that are introduced in VANET include safety, non-safety, and entertainment. The main purpose of the safety applications is the safety of vehicles and passengers, whereas non-safety applications improve the efficiency of VANET. Entertainment applications also include web access and file sharing [3].

VANET is a good context for an attacker to challenge the network with its malicious attacks. In addition, one must ensure that all data sent cannot be injected or changed by users who are malicious [4]. Malicious nodes can use network infrastructure to produce false messages and change or abuse them even in the routing

Doi: 10.22061/JECEI.2019.5125.193

process [5]. Attached information to a packet can make easy the identification process of a vehicle by a malicious node. Securing VANET protocols can resist vehicles against any type of attack. Protocol design and securing private data for drivers is hard and essential work in VANET [6]. In designing a routing protocol, one should look at the temporary network fragmentation and a broadcast storm problem. The main challenge in designing routing protocols is to provide low communication delay, overhead, and complexity [7].

Secure routing protocols focus on providing authentication and path validity. They do not completely address communication securing nor prevent eavesdropping or data modifying. Hosts must still utilize end-to-end cryptography to protect themselves from these attacks. Secure routing cannot detect or prevent packet loss due to attacks [8].

To reduce the effect of attackers, we propose a detection technique that helps to isolate the malicious nodes from a network by using a trust management system. If a node has an unacceptable trust value, other nodes punish it by isolating and it is also forced to behave well. Our contributions to this paper are:

1- Classifying all types of routing attacks and attackers in VANET.

2- Proposing a new framework for secure routing in order to deal with black-hole attacks.

3- Proposing a detection technique that helps to determine and isolate malicious nodes using a trust management system. The proposed system can increase reliability by improving the probability of timely and correct delivery of a safety message. Section 2, we present basic security requirements in VANET. Section 3 classifies all possible attacks and attackers in routing phase of safety message delivery. A new framework for secure routing in VANET is presented in Section 4. Simulation results are discussed in Section 5. At the end, we conclude our paper with the analysis of simulation results and some suggestions for future works in Section 6.

VANET Structure and its Requirements

Exchanging messages between vehicles is done through a Dedicated Short-Range Communication (DSRC) in 5.9 GHz band with 75 MHz channels and IEEE 802.11p technology. It can create simultaneous communications between Road Side Units (RSUs) and vehicles.

Vehicle to vehicle communication allows vehicles to connect with each other over a multi-hop path. A stable connection between vehicles and RSUs can reduce the effect of routing attackers in VANET [9]. So, the main challenge in VANET's routing is to eliminate the disruptive effect of routing attackers. Unknown vehicle addressing is also amongst the main problems having stable communication [10].

Vehicles may establish connections with other vehicles or RSUs to collect traffic information [11]. In RSU to RSU communications, some information for better efficiency will be exchanged. This type of communication plays a vital role in both V2V and V2R communications.

It can authenticate the validity of vehicles [12]. To reach a secure connection in VANET, some security points are required. Table 1 shows the most important cases.

Table 1: Vanet Requirements

Name	Description
Confidentiality	Messages should not be encrypted for anybody like safety and traffic. Confidentiality is used when some nodes want to communicate as a single group and the members of the group are able to decrypt messages [10].
Authentication and integrity	Authentication process ensures each message to verify its origin and maintain it from malicious nodes. Integrity ensures that data cannot be changed or altered by an unauthorized host. Therefore, the contents of the message are reliable [11].
Availability	It guarantees communication between vehicles and distant nodes in bad conditions. That makes the network available to all users [10].
Privacy and anonymity	To realize privacy use, temporary and anonymous keys are constantly changing and each key is used once to maintain the privacy of drivers [12].
Location accuracy	It locates the sent node accurately to avoid the false information that is provided by the enemy about its location to mislead others [4].
Access control	Vehicular access to services that provided by the infrastructure or remote nodes [13].

Attack and Attackers Classification

VANET applications suffer from various attacks that affect system reliability. In a wireless network, every attacker can easily access exchanged information. In order to investigate the relationship between reliability and security, we name and classify some effective attacks in VANET. By discovering the attacker's goals, we divide attacks into two categories: attacks that change or create critical messages.

In Masquerading (impersonation) attack, an attacker can use a fake identity and pretend as another vehicle. The goal of these attackers is to do any legal or malicious activity such as fabricating, changing and replaying a message. Thus, successful implementation of this attack is difficult due to the integrity capability of secure systems. The risk of this attack is minor [4]. In replay, an attacker tries to use a malicious or an unauthorized identity to impersonate a legal user or RSU. The main aim of this attack is to consume bandwidth. VANET architecture usually can't prevent this kind of attack. So, it can be considered as a major attack [14].

In some privacy attacks such as Information Disclosure (ID) attack, the attacker gets some node's sensitive information illegally. In this attack, the malicious nodes act to monitor the target nodes and send some fake messages to neighbors to collect the required data. Identity and location are amongst some stolen information [15].

In Global Positioning System (GPS) spoofing attack, an attacker can produce GPS false data by generating stronger signals than the original GPS. Thus, the attacker makes the nodes to believe that it is in another GPS signal collisions. The risk of this attack is critical [16]. Sometimes, malicious nodes try to produce fake safety messages. They compel other nodes to change their physical path or default route in the routing table. This type of attack is named as Sybil attack.

Detecting Sybil attacks is a critical security problem in VANET [17].

Man In The Middle (MITM) attacks as another minor attack affect the VANET by listening to the communications between two or more unknown vehicles in the network [15].

The aim of this attack is to eavesdrop on communications and use the obtained information and/or inject false information [18]. The attackers may send false information about the geographical location in the beacon messages [19]. This type of attack is also a critical threat in VANET [20].

Tracking vehicles and determining their location can lead to theft or building a profile of the user in the location tracking attack. It impress user privacy and has a major impact on VANET reliability [21]. On the other hand, some attackers inject false messages into the network to cause a dangerous problem in tampering attacks. In this attack, hiding safety messages may lead to an accident. In Denial of Service (DoS) attack, fake messages are injected into the network in order to prevent users from accessing network resources [22].

In a malware attack, attacker inserts some malware into VANET, which causes dangerous disruption. These programs enter into the networks when the OBUs (On Board Units) and RSUs receive periodic software and firmware updates. This attack is a high-risk one. Spamming attackers broadcast spam messages into the network. They can increase delivery message delay and decrease the QOS.

Attackers in the black hole attack creates a region in which no vehicle can propagate the message. A malicious node pretends to have a direct path to a destination node. As a result, they are able to intercept packets or keep them without forwarding and causes data loss. This attack is considered as a critical one [16].

A new classification of famous VANET's attacker is presented in Table 2 according to their extent and strength.

First level attackers have a higher density than the second level. These attackers are active and carry out different types of attacks on the infrastructure, i.e., vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) at the same time. The purpose of these attackers is to make a disturbance in the normal operation of the network without achieving any personal benefits [23], [24]. The main purpose of the second level attackers is to achieve their personal benefits.

Using reference [22], another classification of attackers is presented in Table 3. In general, attackers try to change the contents of the message or create fake messages and use them for their own benefits. Additionally, the level of their affection is determined as high (serious consequences to users or network), medium (short-term outages) and low (minor consequences to users or network). Attacks are also classified into critical, major or minor depending on the probability of their appearance and their impact on the user or the network.

A New Framework for Secure Routing in VANET

Securing VANET is a very difficult task, because of its dynamic nature and a high volume of message overhead. But, routing protocols need to find the safest path between two nodes. It may need to produce and exchange some control messages.

They establish vital routes, discover instant alternative routes in case of the path loss and make some decision about packet dissemination and forwarding [25], [26]. Designing the routing protocol, one should look at the network fragmentation and broadcast storm problems [7].

Secure routing protocols provide origin authentication and validity of the path. Therefore, secure routing does not directly address secure communication and it can't prevent attackers from eavesdropping, modifying data traffic or packet loss due to attacks. Hosts must still use end-to-end cryptography to defend against these attacks [27]. The main standard of successful routing in VANET is to take the shortest and reliable path considering some other environmental parameters such as weather condition, interesting roads and the least expensive route [28].

Table 2: Types of Attackers

Name	Description
First level attacker	• **Insider:** Authorized members who do the malicious activity to disturb the network by changing the certificate keys. These attackers have a stronger impact than others because the attacker from inside is the right person to do the wrong work. • **Malicious:** They have no personal gain but their goal is to confound the other vehicles by sending wrong information or changing the information related to the safety applications. • **Active:** Attackers who generate packets and send it to other vehicles as well as to the infrastructure or generate signals and send it to disturb the main frequency band. • **Extended:** They facilitate extending and spreading attacks across the network.
Second level attacker	• **Outsiders:** They try to enter the network either by identity theft or various attacks. They want to misuse network protocols. • **Rational:** Attackers who seek to achieve their own interest. For example, they send wrong data about the road and change traffic data to clear the road for their benefit. • **Passive:** The attacker feels the network through eavesdropping on the wireless channel between the vehicles and infrastructure of the network. They consider the violation of the privacy of users on the road. • **Local:** Those who are restricted in the scope.

Therefore, the general objective of secure routing protocols is to protect routing messages from attackers who try to modify these messages or inject false routing messages. On the other hand, the safety and authenticity of routing messages must be ensured. Confidentiality may be insured easily, for example by encryption. It may lead to an overhead increase. As a result, the process of establishing a route must be quick. In the case of building many security mechanisms, the efficiency of the routing protocol may be sacrificed. Therefore, it is important to have a trade-off between security and efficiency [25].

At first, we address some important secure routing protocols: Authenticated Routing for Ad-hoc Networks (ARAN) [8], Secure Efficient Ad-hoc Distance Vector (SEAD) [29], A Secure On-Demand Ad-hoc Network Routing Protocol (ARIADNE) [25], Secure Message Transmission (SMT) [30], Secure Ad-hoc On-Demand Distance Vector (SAODV) [31].

The ARAN protocol is considered as an on-demand secure routing protocol (AODV). ARAN provides authentication of route discovery and message integrity [8]. The main goal of ARAN is to detect misbehaviors and protect the network against their actions. This protocol delegate authentication, integration and repudiation management to security policies [25].

SEAD is a proactive secure routing protocol that protects the network from uncoordinated attackers which may send incorrect routing messages to other nodes. SEAD depends on the Destination-Sequenced Distance-Vector (DSDV) and uses hop-by-hop security mechanisms. It periodically exchanges the routing information by other nodes. In this way, every node constantly knows the current route for all destinations [29]. SMT is a secure protocol for end-to-end data transmission and guarantees a stable connection in a network with dynamic topology.

Secure on-demand Ad-hoc network (ARIADNE) routing protocol is based on dynamic source routing (DSR) that uses a highly efficient symmetric cryptography [25]. Security in ARIADNE follows an end-to-end approach. ARIADNE supposes the presence of a common secret key between nodes and utilizes the message authentication code (MAC) for authenticating messages between nodes [32].

SAODV is a security extension of the AODV protocol, based on public key cryptography. SAODV routing messages are encrypted by a digital signature to ensure their integrity. The security features provided by SAODV include integrity, authentication, and non-repudiation [33].

So, the proposed framework for secure routing in VANET considers all types of attacks and attackers in order to decrease the effectiveness of their misbehaviors on the reliability of VANET. This framework is presented in Fig. 1.

Wireless access in vehicular environments (WAVE) includes two IEEE 802.11p and IEEE 1609 family protocols. IEEE 802.11p involves WAVE and functions primarily at the PHY and MAC layers. IEEE 1609.1 defines some services and interfaces of WAVE for resource manager application.

IEEE 1609.2, a security service, ensures the security of messages exchanged in WAVE. It aims to achieve authentication, data verification, non-repudiation, and privacy protection against eavesdropping, spoofing, alteration, and replay. IEEE 1609.3 specifies the operation of addressing and routing services in network and transport layers in order to secure data exchange. IEEE 1609.4 is an enhancement to the 802.11 WAVE support [34].

Table 3: Attacks Analysis

Type of attacks	Communication type	Classes of attack	Threat level	Security requirement	Type of attacker	Impact of attacks	Risk
Masquerading & Impersonation	V2V	Data Link, Network, Transport, Application	Less-medium	Authentication Integrity	Insider, Malicious, Active, Local	High	Minor
Replay attack	V2I	Data Link, Network, Transport, Application	Less-medium	Authentication Non-repudiation	Insider, Malicious, Active, Local	High	Minor
ID disclosure attack	V2V V2I	Network	Less-low	Authentication Privacy	Insider, Rational, Active, Local	High	Major
GPS spoofing	V2I	Application	Less-medium	Authentication	Outsider, Malicious, Active, Local	High	Critical
Sybil attack	V2V V2I	Data Link, Network, Transport, Application	Less-medium	Authentication	Insider, Malicious, Active, Local	High	Major
MITM attack	V2V	Physical , Data Link, Network, Transport, Application	Low	Confidentiality Authentication Non-repudiation Integrity	Insider, Rational, Active, Local	High	Major
Injection of false information	V2V V2I	Application	Medium	Authentication Availability	Insider, Rational, Active, Local	High	Major
Location tracking	V2V V2I	Application	Less-low	Privacy	Outsider, Malicious, Passive, Local	High	Critical
Broadcast tampering	V2V V2I	Application	High	Availability	Insider, Malicious, Active, Local	High	Minor
DoS attack	V2V V2I	Physical ,Data Link, Network, Transport, Application	High	Availability	Insider, Malicious, Active, Local	Medium	Major
Malware	V2I	Application	High	Availability Confidentiality Integrity	Insider, Malicious, Active, Extended	High	Critical
Spamming	V2I	Application	High	Availability	Insider, Malicious, Active, Extended	Low	Minor
Black hole attack	V2V	Network	High	Availability	Insider, Malicious, Passive, Local	High	Critical

Whereas mobility management is used to gives the best connectivity for mobile nodes in the ad-hoc networks [35]. Another solution for increasing reliability in VANET according to calculation of vehicle's transmission range and keeping communication is presented in [36].

The secure, routing module is responsible for some mechanisms against misbehaviors in the routing process. It should identify a specific attack and neutralize its effects. Since the black-hole attack is an annoying attack in VANET, we propose a new secure routing protocol to overcome the effect of this attack.

It affects mainly on AODV protocol because it doesn't contain any security mechanisms to ensure that the packets have reached the destination. Attackers can advertise themselves as a relay node to all destinations.

They may deceive others to transmit their packets to them to cause damage to them.

The proposed detection technique helps normal nodes to isolate the malicious nodes from others using a trust management system. The proposed algorithm is presented in Fig. 2.

The trust value of nodes changes in two phases. In the first phase, each node broadcasts an RREQ message to others. Regarding the behaviors of nodes in forwarding messages, their trust values may change by the sender. In the second phase, after updating trust values, packets will be sent to other nodes from the path with the highest trust values. This process can repeat on demand.

Initially, each node broadcasts a HELLO message to evaluate the honesty of its neighbors forwarding the message. When the source node wants to send a safety message to a destination, it will specify the established route and broadcast RREQ message in a narrow direction according to destination node location.

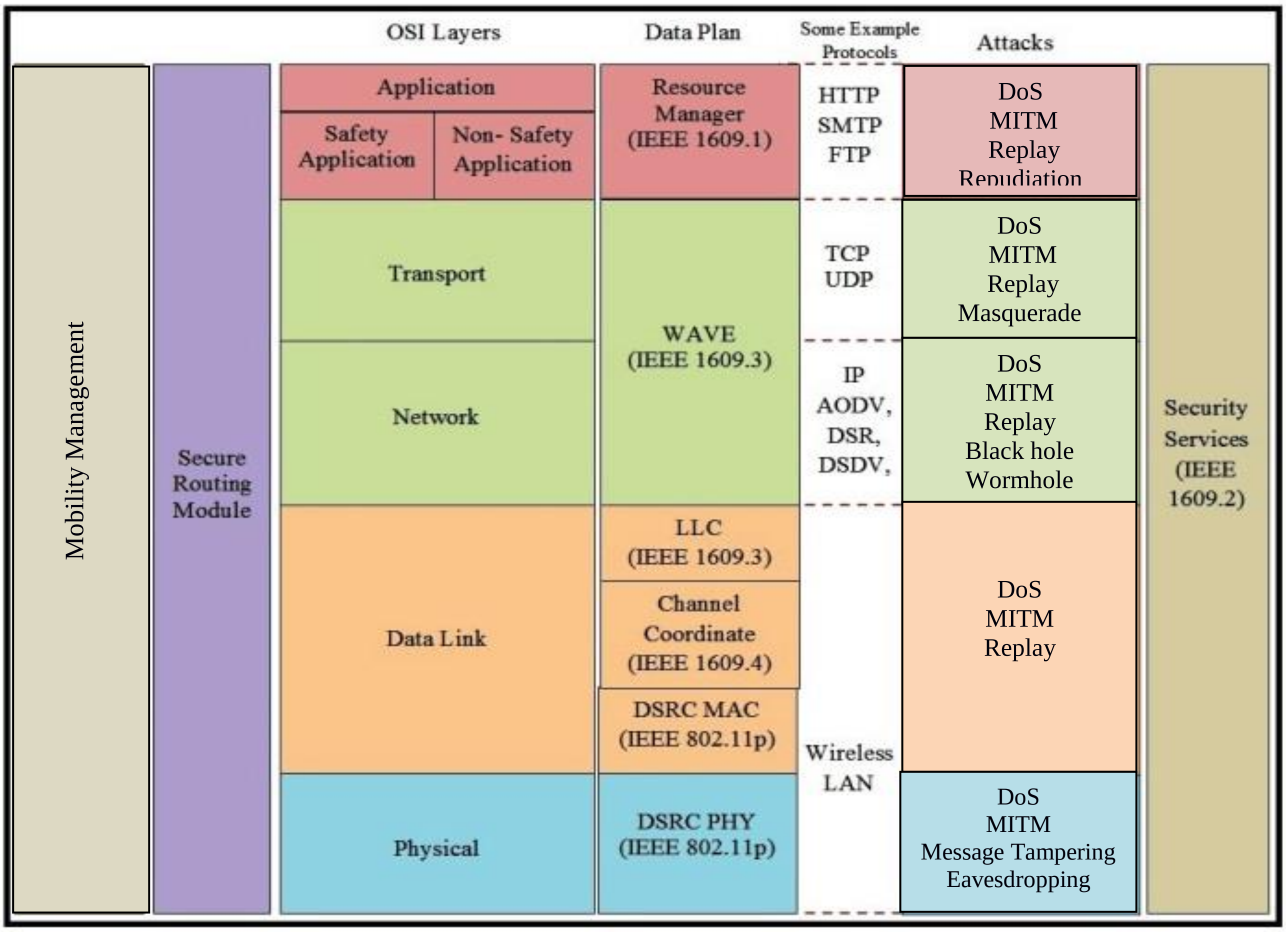

Fig. 1: Proposed framework for secure routing.

The intermediate node that receiving RREQ will verify the request whether it is a destination or not. If it is a destination node, it replies with an RREP message, otherwise, the RREQ packet will be forwarded to other neighbor nodes and so on.

After obtaining a trust stamp by intermediate nodes, they can send packets to the destination. Nodes that couldn't get the trust stamp will be listed in the blacklist, which will not use in message forwarding for a period of the time.

Simulation Results

In order to evaluate the proposed secure routing protocol, some simulations are conducted in NS-3.28. The performance results are analyzed based on throughput and packet receiving rate.

```
BEGIN
Step 0: Allocate a primary trust value to each node in range
        [0..1]
Step 1: Source node sends RREQ to all its neighbours.
Step 2: Intermediate nodes forward RREQ to destination
        address.
Step 3: Intermediate nodes sends RREP message to source
        node.
Step 4: If there exist any direct path to destination:
                Send your packet immediately to it.
        Else,
                We have some path with different trust
                values (some of them contain malicious
                nodes) go to STEP 7.
Step 5: Rout from source to destination established.
Step 6: Source node stores next hop.
Step 7: Check trust value of nodes in old and new paths.
        If ((oldPathAvgTrustValue < Threshold) &&
        (newPathAvgTrustValue >= Threshold))
          Discard the old path and go to Step 5.
        Else if ((oldPathAvgTrustValue < Threshold) &&
        (newPathAvgTrustValue < Threshold))
        Choose a path with the highest trust values and go to
        Step5.
```

Fig. 2: Suggested algorithm for preventing black hole attack using a trust management system.

The total simulation time is 100 seconds for 100 nodes with 10%, 20%, 30%, and 40% black-hole attack.

We evaluate our proposed protocol by considering two different scenarios: Routing with and without a trust management system. In both scenarios, 100 moving nodes with a constant speed of the 20 meters per second with 10%, 20%, 30%, and 40% malicious (with black-hole attack) in a simulation area with 1500 × 1500 meters are considered.

Scenario 1: The first simulation scenario is built to measure the network performance in the presence of a black-hole attack. These malicious nodes are placed on the network between the sender and the receiver. This malicious nodes drop all routing packets.

Scenario 2: Our goal is to show the effect of using a trust management system on securing the routing protocol and increasing the reliability. Random mobility is selected with an average speed of 20 meters per second.

Sending data rates is 11 Mbps with a transmitting power of 7.5dB. In this scenario, 10% of the nodes are malicious.

Vehicles broadcast 400-byte packets at a rate of 50 times per second. In addition, each vehicle has a maximal transmission range set to 500m. Fig. 3 shows the default scenario.

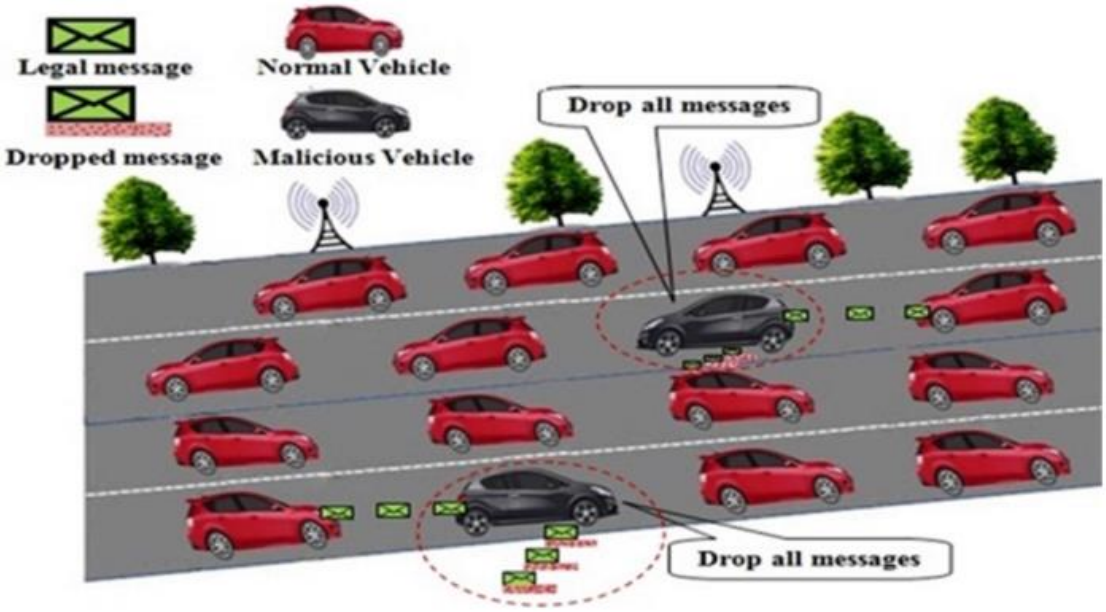

Fig. 3: Default scenario for Highway.

The simulation parameter's values are introduced in Table 4. The measured throughput is presented in Fig. 4 as kbps. Results are compared to AODV in the existence of the malicious nodes. The vertical axis shows the percentage of malicious nodes and the horizontal one is throughput.

For the proposed protocol, the average throughput has higher performance because it can decrease delay and minimize the number of hops in the selected path. Throughput will decrease a little in the case of 20%, but this does not affect the performance of the proposed protocol.

Table 4: Simulation Parameters

parameter	value
simulator	ns-3 (var. 3.28)
number of nodes	100
malicious nodes	10%, 20%, 30%, 40%
simulation time	100 sec
simulation area	1500 × 1500 meter
wave packet size	400 bytes
sent data rate	2048 bps (2.048 kbps)
mobility model	random way point mobility model
routing protocol	myaodv routing
node speed	20 m/s (70 km/h)
pause time	0 sec (no pause time)
transmit power	7.5
propagation model	two ray
frequency	5.9 ghz
mac protocol	ieee 802.11p
transmission range	500 m

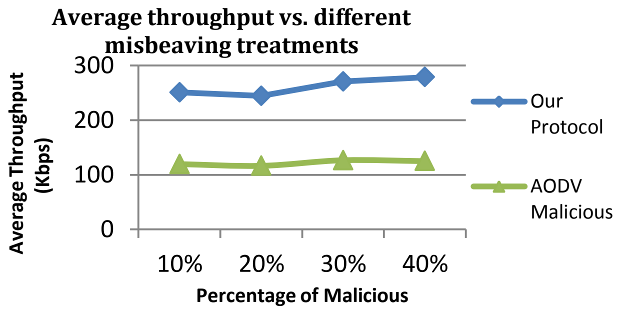

Fig. 4: Average Throughput in proposed protocol.

Throughput in AODV decreases in the presence of malicious nodes because we lose some routing packets retransmits them. The receiving packet rate is shown in Fig. 5.

The proposed protocol provides higher receiving rates than AODV because packets are transmitted on reliable paths.

In AODV with malicious nodes, some routing packets will be ignored in the selected path and delay will increase.

Due to this delay, packets form a queue at nodes which may lead to node failure and packet loss. Thus, the proposed protocol has a better packet receive rate than AODV with the presence of a malicious node.

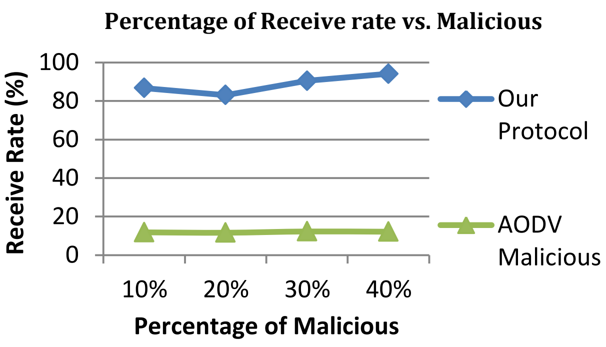

Fig. 5: Average receive rate in proposed protocol.

Conclusions

Today, VANETs are used in various countries to increase the road safety. Ensuring the security and accuracy of exchanged packets are among the main necessity of VANET.

Securing a route in VANET in order to increase the reliability of that is amongst the main challenging subjects. So, in this paper, a new protocol for routing and identifying various misbehaviors is proposed based on this framework.

The proposed routing protocol isolates malicious nodes from the network by using a trust management system. Having investigated AODV with a black-hole attack, it was observed that the network throughput and packet receive rate decreased significantly in the presence of attackers. The black-hole attack affects the entire VANET connectivity. It decreases the packet receiving rate.

Our simulation results show that the proposed protocol can overcome the effects of black-hole attackers and it can increase throughput by 93% and packet received rate by 94.14% compared to the original AODV.

Investigating the effect of the other attacks, simulating in an urban area with repetitive communications and considering the RSU in verifying the trustworthiness of entities are suggested for our future works.

Author Contributions

S. Goli-Bidgoli and M. Sofar-Ali designed the experiments. M. Sofar-Ali collected the data. S. Goli-Bidgoli carried out the data analysis. S. Goli-Bidgoli and M. Sofar-Ali interpreted the results and wrote the manuscript.

Acknowledgements

Authors are grateful to University of Kashan for supporting this work by Grant No. 891105.

Conflict of Interest

The authors don’t hafe any conflict of interests regarding the publication of this manuscript.

Abbreviations

VANET	Vehicular Ad-Hoc Networks
MANET	Mobile Ad-Hoc Networks
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
DSRC	Dedicated Short-Range Communication
RSU	Road Side Units
ID	Information Disclosure
GPS	Global Positioning System
MITM	Man In The Middle
OBU	On Board Unit
DSDV	Destination-Sequenced Distance-Vector

References

[1] S. U. Rehman, M. A. Khan, T. A. Zia, L. Zheng, "Vehicular Ad-Hoc Networks (VANETs) - An overview and challenges," J. Wirel. Netw. Commun., 3(3): 29–38. 2013.

[2] S. Goli-Bidgoli, N. Movahhedinia, "A trust-based framework for increasing MAC layer reliability in cognitive radio VANETs," Wirel. Pers. Commun., 95(3): 2873–2893, 2017.

[3] V. Kumar, S. Mishra, N. Chand, "Applications of VANETs: present & future," Commun. Netw., 5(1): 12–15, 2013.

[4] M. S. Al-kahtani, "A survey on security in vehicular Ad Hoc networks," in Proc. 2012 6th Int. Conf. Signal Process. Commun. Syst. (ICSPCS), 4(1): 1–9, 2012.

[5] F. Al-Hawi, C. Yeun, M. Al-Qutayti, "Security challenges for emerging VANETs," presented at the 4th Int. Conf. Inf. Technol., Jordan, Amman, 2009.

[6] P. Golle, D. Greene, J. Staddon, "Detecting and correcting malicious data in VANETs," in Proc. first ACM Work. Veh. Ad Hoc Networks VANET: 29–37, 2004.

[7] S. H. Cha, "A survey of greedy routing protocols for vehicular Ad Hoc networks," Smart Comput. Rev., 2(2): 125–137, 2012.

[8] S. Mehla, B. Gupta, P. Nagrath, "Analyzing security of authenticated routing protocol (ARAN)," Int. J. Comput. Sci. Eng., 02(03): 664–668, 2010.

[9] R. Kumar, M. Dave, "A review of various VANET data dissemination protocols," Int. J. Sci. Technol., 5(3): 27–44, 2012.

[10] U. Parmar, S. Singh "Overview of various attacks in VANET," International Journal of Engineering Research and General Science, 3(3, 2015.

[11] P. Papadimitratos, V. Gligor, J. P. Hubaux, "Securing vehicular communications-assumptions, requirements, and principles," Work. Embed. Secur. Cars: 1-10, 2006.

[12] H. Hasrouny, A. E. Samhat, C. Bassil, A. Laouiti, "VANET security challenges and solutions: A survey," Veh. Commun., 7: 7–20, 2017.

[13] B. Mokhtar, M. Azab, "Survey on security issues in vehicular Ad Hoc networks," Alexandria Eng. J., 54(4): 1115–1126, 2015.

[14] K. Amirtahmasebi, R. Jalalinia, "Vehicular networks – security, vulnerabilities and countermeasures," Master Sci. Thesis Progr. Networks Distrib. Syst. Chalmers Univ. Technol.: 1–55, 2010.

[15] S. Santosh, R. Sharma, "VANET: Security attacks and its possible solutions," J. Inf. Oper. Manag., 3(1): 301–304, 2014.

[16] S. Zeadally, R. Hunt, A. Irwin, A. Hassan, "Vehicular Ad Hoc networks (VANETS): status, results, and challenges," Telecommun. Syst., 50(4): 217–241, 2010.

[17] T. Zhou, R. R. Choudhury, P. Ning, K. Chakrabarty, "P2DAP sybil attacks detection in vehicular Ad Hoc networks," IEEE J. Sel. Areas Commun., 29(3): 582–594, 2011.

[18] P. G. Jose, S. Chatterjee, M. Patodia, S. Kabra, A. Nath, "An effective review on attacks in vehicular ad hoc networks," Int. J. Innov. Res. Comput. Commun. Eng., 4(9): 2257–2263, 2016.

[19] C. Harsch, A. Festag, P. Papadimitratos, "Secure position-based routing for VANETs," in Proc. IEEE Veh. Technol. Conf.: 26–30, 2007.

[20] G. Saranya, P. Nathiya Devi, T. Amitha Raghu, "Data confidentiality and users' location privacy in VANETs," International Journal of Engineering Development and Research, 2(2): 1391–1397, 2014.

[21] J. M. De Fuentes, A. I. González-Tablas, A. Ribagorda, "Overview of security issues in vehicular Ad-Hoc networks," in Handbook of Research on Mobility and Computing, IGI Global, 894–911, 2011.

[22] V. H. La, A. Cavalli, "Security attacks and solutions in a vehicular Ad Hoc networks : A survey," Int. J. Ad Hoc Netw. Syst., 4(2): 1–20, 2014.

[23] R. S. Raw, M. Kumar, N. Singh, "Security challenges, issues and their solutions for VANET," Int. J. Netw. Secur. Its Appl., 5(5): 95–105, 2013.

[24] S. Kumar Biswal, "Onboard unit based authentication for V2V communication in VANET," Natl. Inst. Technol.: 1–46, 2014.

[25] Y. C. Hu, A. Perrig, D. B. Johnson, "Ariadne: A secure on-demand routing protocol for Ad Hoc networks," Wirel. Networks, 11(1–2): 21–38, 2005.

[26] D. Yan, "Routing and security in vehicular networking,".

[27] O. In, H. Hartenstein, K. P. Laberteaux, "A tutorial survey on vehicular Ad Hoc networks," Commun. Mag. IEEE, 46(6): 164–171, 2008.

[28] A. Hassan, S. Zeadally, R. Hunt, A. Irwin, Y. S. Chen, "Vehicular Ad Hoc networks (VANETS): Status, results, and challenges," Telecommunication Systems, 50(4): 217–241, 2010.

[29] V. Patel, "A survey paper of bellman-ford algorithm and dijkstra algorithm for finding shortest path in GIS application," Int. J. P2P Netw. Trends Technol., 5: 1–4, 2014.

[30] S. Erotokritou, "Secure message transmission and its applications," Doctoral dissertation, UCL (University College London), 2016.

[31] V. Singh, M. Jain, "Secure AODV routing protocols based on concept of trust in MANETs," Int. J. Adv. Res. Comp. Eng. Tech. (IJARCET), 3(12): 4425–4428, 2014.

[32] Y. C. Hu, A. Perrig, D. B. Johnson, "Ariadne: A secure on-demand routing protocol for Ad Hoc networks," Wirel. networks, 11(1–2): 21–38, 2005.

[33] M. G. Zapata, N. Asokan, "Securing Ad Hoc routing protocols," in Proc. of the 1st ACM workshop on Wireless security): 1–10, 2003.

[34] Y. J. Li, 2012, "An Overview of the DSRC / WAVE Technology," Qual. Reliab. Secur. Robustness Heterog. Networks: 544–558.

[35] V. Kumar, P. K. Dahiya, "Mobility management in vehicular adhoc networks : a review," IOSR Journal of Electronics and Communication Engineering, 11(1): 85–96, 2016.

[36] S. Goli-Bidgoli, N. Movahhedinia, "Determining vehicles' radio transmission range for increasing cognitive radio VANET (CR-VANET) reliability using a trust management system," Comput. Networks, 127): 340–351, 2017.

Biographies

Salman Goli-Bidgoli received his B.Sc. from Kashan University, Iran in 2008 and his M.S. and Ph.D. from the University of Isfahan, Isfahan, Iran respectively in 2011 and 2017 in Computer Architecture Engineering. He is the author of several technical papers in Computer Networks and Telecommunications journals and conferences. He is the assistant professor of the Computer Engineering Department of Kashan University, Iran. His research interests are Wireless networks, Reliability, Internet of Things and Block-chain.

Mays Mousa SofarAli received her B.Sc. from Kufa University, Iraq in 2009 and her M.Sc. from the University of Kashan, Kashan, Iran in 2018 in Computer Engineering. Her research interests are Wireless networks and Security.

How to cite this paper:

S. Goli-Bidgoli, M. Mousa SofarAli, “A New Framework for Secure Routing In VANET,” Journal of Electrical and Computer Engineering Innovations, 6(2): 119-128, 2018.

DOI: 10.22061/JECEI.2019.5125.193

URL: http://jecei.sru.ac.ir/article_1097.html