Provision of Security in Vehicular Ad hoc Networks through An Intelligent Secure Routing Scheme

Kashif Naseer Qureshi[1]
[1]Computer Science Department, Bahria University, Islamabad, Pakistan
E-mail: kshifnq@gmail.com

Faisal Bashir[1], Abdul Hanan Abdullah[2]
[2]Faculty of Computing, University Teknologi Malaysia, Skudai, Johor Bahru, Malaysia
hodcsib@bahria.edu.pk, hanan@utm.my

***Abstract*— Vehicular Ad hoc Networks (VANETs) are providing road management systems by a wide variety of different value-added safety and infotainment applications. The main aim of these networks is to provide data communications among vehicles with or without infrastructure. Due to advancements and wide deployment of wireless technologies in these networks, different types of security attacks and malicious abuses may lead to catastrophic results in the networks. In this paper, we propose an Intelligent Secure Routing Scheme (ISRS) to secure the data communication with or without infrastructure especially for emergency messages propagation. Simulation results indicate the superiority of proposed scheme on data security in the presence of malicious nodes activities in the network.**

***Index Terms*— Security, VANETs, Scheme, Road side unit, Signal Strength, Distrust, Security**

I. INTRODUCTION

Vehicular Ad hoc Networks (VANETs) have attracted extensive attention due to its plethora of data communication services in the transportation sector. These networks provide ubiquitous wireless communication among vehicle nodes and improve passenger's safety by traffic management. This trend has boosted and now every vehicle manufacturing industry has focused to equip their vehicles with advanced communication technologies and bring Internet services in vehicles [1, 2]. The applications in VANETs are categorized into two main types safety and infotainment. Safety applications have very critical information. In these applications, in any case' data should be delivered in time to prevent the serious impact on the roads such applications are accident detection, weather warning and curve alert. On the other hand, in infotainment applications' the data requires normal transmission such as in file sharing, advertisement and the Internet applications. Due to the rapid growth of VANETs applications and open communication systems, security is one of the significant concern, especially for safety applications. Data authentication, non-repudiation and integrity are the main requirements of safety applications [3]. Due to the high mobility of vehicle nodes and dynamic network topologies, different types of security attacks and vulnerabilities exist in safety applications.

In terms of security, malicious node attack, denial of services, impersonations are the common attacks in the network. In vulnerabilities, violation of privacy, forgery is some other examples [4]. In order to address these security concerns, various different type of solutions have been made to ensuring the security of sensed data. In addition, these security concerns also bring privacy as another concern where the sensed data could reveal the personal information of the vehicle. In addition, the vehicle location is another security concern which is linked with travelers [5]. Denial of services is another active attack which tries to down the network for criminal purposes such as inject some false information to jam the radio communication in the network [6]. In addition, the attackers also inject bogus information about traffic congestion during data communication to divert the driver attention for any purpose. Privacy is also suffered due to unsecured data routing where the attacker can listen to the channel and persuade the user to be a part of their communication such as sinkhole and wormhole attacks [7]. All data communication in these networks requires that the sharing information sent or received must be secure. Otherwise, the security attack on this data transmission has a serious impact on the network. Therefore, there is a need to design a diverse routing protocol to secure the data and prevent the network from possible attacks.

Based on above security challenges in VANETs, we propose an Intelligent Secure Routing Scheme (ISRS) to provide data security during data transmission. This scheme secures the data from malicious attacks in the network and assures the data security during data transmission. Proposed scheme reduces the communication overhead and more suitable for dense and sparse dynamic and ephemeral VANETs.

0-7695-6347-3/17/$31.00 ©2017 IEEE
DOI 10.1109/FIT.2017.00043

The rest of the paper is organized as follows. Section 2 presents the related work in detail and discusses existing security schemes and their advantages and weaknesses for the motivation of our work. Section 3 presents the proposed scheme design, assumptions, and architecture. Section 4 discusses the performance evaluation of proposed scheme and simulation results in terms of data delay, throughput, and detection ratio. Section 5 sums up the paper with future direction.

II. Related Work

Various different types of security and privacy schemes have proposed to tackle the security preservation in VANETs. In this section, we discuss some existing schemes and generalize their advantages and limitations.

A scalable robust secure routing scheme was proposed in [8] to address the certificate distribution, avoidance and revocation issues in VANETs. This scheme is based on Road Side Unit (RSU) where vehicle nodes maintain a group within its transmission range and broadcast messages to verifying the other vehicles in the same group. In addition, whenever the message is found to be false, a third party can be raised to open the vehicle nodes identity of message originator in the network. In this research, vehicle nodes only send the request message with a new secret key when vehicles pass by RSUs and expire their secret member keys. Every vehicle node verifies messages when they pass through RSUs. This scheme reduces the certificate management overhead. However, the VANETs environment is very complex in terms of different obstacles in urban areas such as buildings, trees, and heavy vehicles. These obstacles deplete the data communication and authentication process among vehicles and RSUs. Author ignored this aspect in this work which has a serious impact on vehicular communication.

Lightweight and scalable routing scheme called Privacy Preserving Detection of Abuses of Pseudonyms (P2DAP) to address the Sybil attack was presented in [9]. In this scheme, vehicle nodes detect the malicious activity by passive overhearing through fixed RSUs. For the design of this scheme, author assumed some assumptions where the department of the motor vehicle always facilitates traffic routing, maintain vehicle record and generates pseudonyms. Whenever an attacker carries out Sybil attack by multiple pseudonyms in VANETs, scheme adopts a baseline method to forwards the data to the department of motor vehicle to examine the signature of each message. If department observes that any vehicle has two different pseudonyms, its mean there is an attack. The proposed scheme handles this load through RSUs to reduce this load from vehicle department and releasing only limited amount of information by using hash collusions. Authors claimed that in this distributed method' the network will be more secure and efficient to handle Sybil attack in the network. However, this scheme only distrusted a load of departments into RSUs which has not a significant contribution and has a minor impact in the network.

An authentication key establishment scheme based on IPv6 road networks was proposed in [10]. In this scheme, a mobile vehicle obtains a unique address from other neighbor vehicles or RSUs without duplicate address detection. This scheme has cryptography authentication method based on zero knowledge proof in which every node used to convince another node on the possession of certain secret without revealing and allows encrypted communication during authentication. Basically, this scheme has three main steps, the first step is providing anonymous authentication where a message issuer authenticate itself. In the second step, the scheme provides communication secrecy for confidentiality. In the last step, scheme achieves low storage requirements where fast message verification and cost-effective identity tracking provides in case of any dispute. However, due to the high mobility of vehicle nodes in the network, the mobile vehicle is not fulfilling these protocol requirements which leads to redundant address detection during obtaining unique addresses from neighbor nodes.

Another secure and privacy preserving scheme was proposed in [11] for VANETs to address cheating attacks launched by selfish and malicious on board units. Basically, in this work' author suggested a small tamper-proof hardware module called Trlns's which is attached with on board unit for unique counter identity. However, hardware solutions are not suitable for security because the hardware base security is not reliable in terms of scalability. Lightweight and Efficient authentication scheme (LESPP) was proposed in [12] based on self-generated pseudo identity to guarantee the privacy in the network. In the context of lightweight, this protocol uses symmetric encryption and message authentication code for message verification. The author claimed that this scheme addresses the denial of service attack and provides strong privacy where adversaries cannot trace any vehicle node.

After reviewed existing security schemes, it is clear that still VANETs needs some intelligent security scheme specially to handle malicious vehicles disturbance in the network.

III. Proposed Security Scheme

In this section, we discuss proposed security scheme ISRS and its operation. The proposed scheme provides authentication, data integrity, confidentiality and non-repudiation in the network. The main security threats cover by proposed scheme are forging, modification, replay attacks in VANETs. The traditional cryptography schemes are not suitable due to dynamic nature of VANETs. In these schemes, the main issue is to establish the one-way key chain management in the

presence of high mobility of vehicle nodes. The proposed scheme is working with or without RSUs to provide a security in the network.

A. Assumptions

Before describing the design model of proposed scheme, it is worthwhile to discuss some assumptions of the network. We assume the following assumptions:

- All sensor nodes have equal transmission range.
- All sensor nodes are aware of their location information.
- All vehicle nodes are security curious and try to achieve the security requirement.
- RSUs do not have any resource constraints.
- All vehicle nodes are homogeneous with same computing capabilities.

B. Design Overview

RSUs already act as third parties called Certificate Authorities (CAs) for identities management. These CAs are responsible for verify the misbehavior reports and provide a list to Cluster Head (CH) vehicles in the network. Every vehicle node has a white list provided by its respective CH and also has a black list of malicious nodes. In proposed scheme, the vehicle nodes maintain public and private key pairs and update their received messages percentage and evaluate the results and process further. Proposed scheme has the ability to validate the received messages probability through white list received from CH. All messages control by a timer mechanism where messages waiting time is set and after some time interval messages automatically removed. Whenever any message is bogus, it will discard and remove.

Cluster head selection criteria: CHs are selected to verifying the other nodes behavior on the basis of distrust value. The distrust value measures by the trustworthiness of vehicle nodes and less value have more trust compare to misbehavior node. This value is increasing for CH selection. The second criterion to select CH is the signal strength of vehicle node. Better signal strength will have greater chance to be a CH as a verifier in the network.

Message Validation Process: In this process, the messages are validated based on public key certificate including pseudonyms. Whenever, any vehicle node receives a message for its one hop neighbor node with message signature. It will check the message signature verification probability from CH vehicle and validate the message. On the other hand, if any vehicle will not verify the message it will wait for predefined time and then declare invalid message.

Accusation Check: In order to verifying the messages in the network, every vehicle node plays a role and verifying the messages behavior such as received, duplicate and drop messages from neighbors nodes. If any node in the network does not forward a received data packet or send its duplicate copies after a predefined time, it is considering as abnormal node and it will verifying through 1 unit to other vehicle nodes. This value informs to other vehicles and they update their table accordingly.

C. System Model

In our proposed security scheme, the security provision is provided through vehicle-to-vehicle and vehicle-to-RSU communication. RSUs act as a third party to update the CAs in the network. As illustrated in Figure 1, there is a yellow car as a malicious node which wants to disturb the data communication among other vehicles (Green color).

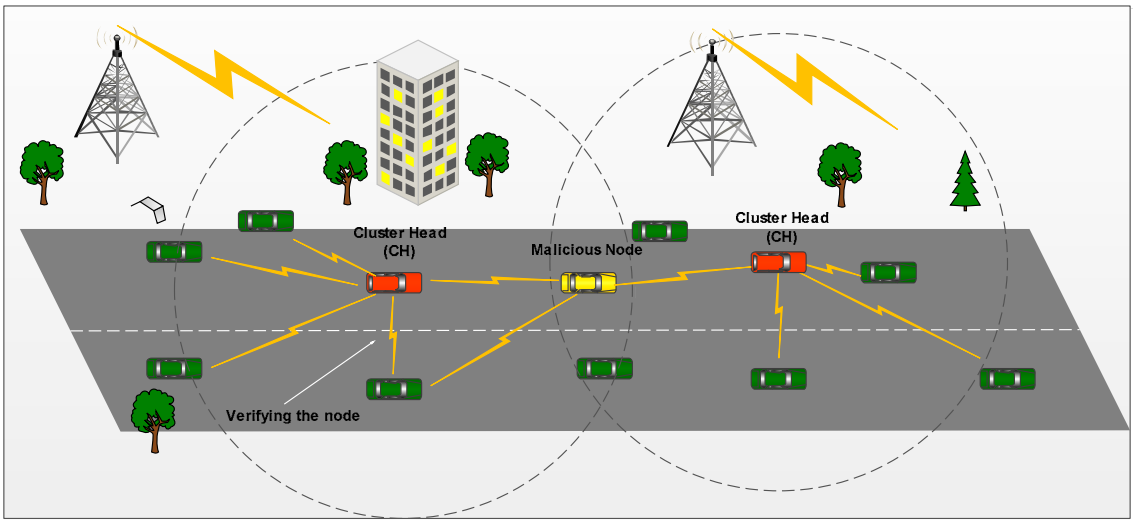

Fig. 1. Data communication in VANETs

CH vehicles are selected on the basis of signal strength and distrust values and monitor the all vehicle behavior within its transmission range and also monitor malicious vehicle (Yellow color) and update other vehicle nodes about its presence. Other vehicle nodes are alert and report this vehicle as a malicious node. By our proposed security scheme, the network will secure from malicious nodes and maintain the data flow in the network.

D. ISRS Algorithm

Algorithm 1 shows the detail operation of proposed security scheme. In the first stage, all vehicle nodes update their location, velocity and distance information through small beacon messages in the network (line 1). Afterward, the CH selection initiates by a best signal strength and distrust values and higher score vehicle node will be CH in specifies region (line 2 to 4). Then, CH informs all other one hop neighbor about its selection (Line 5). If any vehicle node observes any its neighbor misbehavior, it will inform to CH and replies after verification of this node and assigns distrust value to that node (Line 6-8). In last, CH isolates the malicious node and adds it to the black list (Line 10). If there is no malicious node in the network, all vehicle nodes disseminate the data and transmit the packets in the network and exit (Line 11-15).

Algorithm 1

1: Initialize the location information
2: Get the cluster keys
3: Select the CH by Signal Strength and Distrust Value
4: Calculate the parameter and select the node with higher factor node as CH
5: Send the data packet to all neighbor vehicles to inform about CH
6: **if** any vehicle detects abnormal behavior of node
7: Report to CH
8: CH calculates new distrust value of malicious node
9: Isolate the malicious node from the network
10: Update the entry of malicious node and add on black list
11: **else**
12: Monitor the vehicles
13: transmit the packet in the network
14: **end if**
15: **exit**

IV. Performance Evaluation

In this study, we evaluate the performance of ISRS for VANETs. We use NS-2.34 simulator and SUMO mobility model to generate the traffic for evaluating the ISRS performance with or without security schemes. Simulation parameters used in the simulation are listed in Table 1. In the first scenario, we simulate the traffic in the presence of malicious node without any security mechanism and with one existing security mechanism P2DAP to detects the malicious data in the network as shows in Figure 2.

TABLE I. Simulation Parameters

Parameters	Values	Parameters	Values
Simulation area	300 × 300 m	Total number of vehicle nodes	50
Vehicle velocity	11-50 km/h	MAC protocol	IEEE802.11
Transmission range	300 m	Simulation time	400 Sec
Traffic type	CBR	Channel type	Wireless
CBR	512 Kbps	Propagation model	Two-Ray Ground

In first scenario, the vehicle nodes are communicating with each other and share the data for different types of applications. In order to evaluate the security mechanism, we added some malicious vehicles to disseminate the information in the network. The graph result clearly indicates that network has less delay when we implement the ISRS in the network compared to P2DAP and without any security mechanism. In P2DAP scheme, vehicle nodes detect the malicious activity by passive overhearing through fixed RSUs. This scheme only distrusted a load of departments into RSUs and due to this method, it is not working well and cause of delay in the network. The proposed ISRS scheme has better results even though with more data frames in the network.

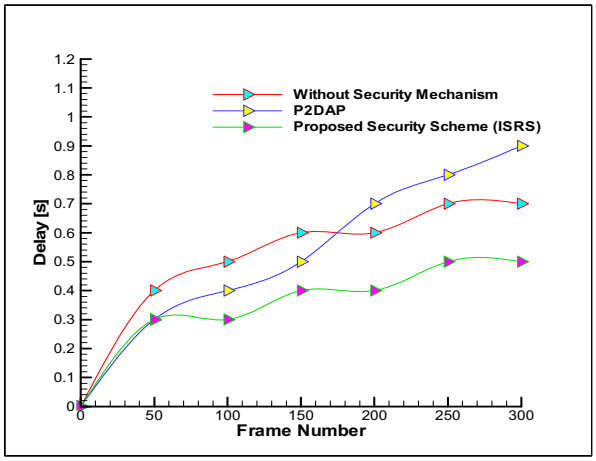

Fig. 2. Data Delay with or without security scheme

After evaluating the results with or without malicious data in the network and compare the results in terms of delay. The results in Figure 3 indicates that the network has suffered from throughput issues in the presence of malicious data and without any security mechanism in the network. The result indicates that due to ISRS, the throughput is high compared to existing scheme P2DAP and without any security mechanism because malicious nodes disturb the network delay and

throughput respectively. Malicious node injects the false or wrong information in the network and in some cases, they will execute the file which has taken more computational power which leads to less throughput and more delay in the network. On the other hand, the existing scheme P2DAP detects the malicious activity by passive overhearing through fixed RSUs and only distrusted a load of departments into RSUs and not working well and has negative impact on throughput.

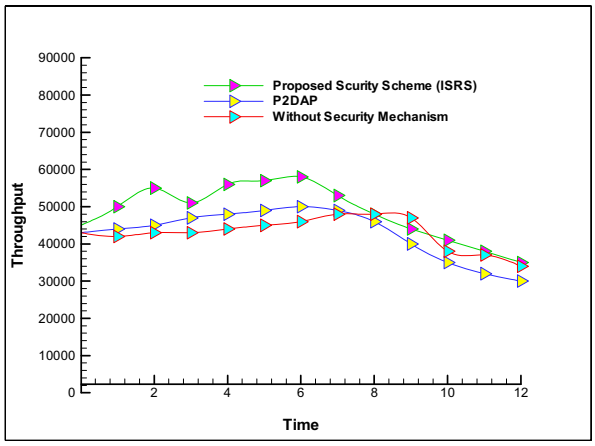

Fig. 3. Data throughput with or without security mechanism

In order to check the effectiveness of our proposed security scheme ISRS to detecting malicious vehicles and determine the detection ratio with or without security scheme. Figure 4 clearly indicates the increment with an increase of task numbers. On the other hand, the results are decreasing rapidly without security mechanism in the network. The malicious nodes inject false information in the network which has direct impact on data dissemination. The existing scheme P2DAP also has better results but still behind the proposed ISRS scheme. Safety applications messages need priority and security in VANETs and need special care to secure the data without any delay with high throughput.

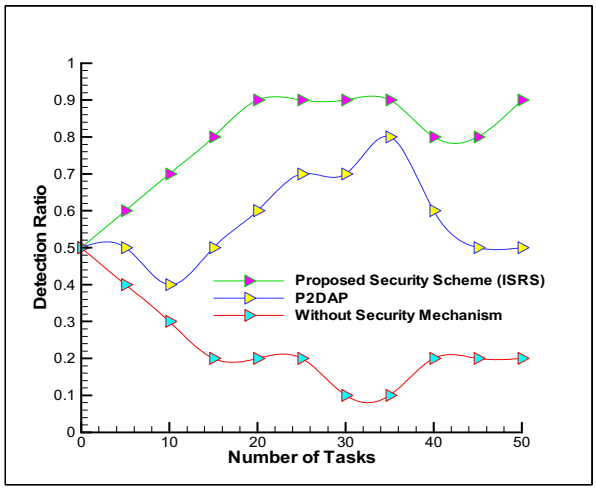

Fig. 4. Detection Ratio with or without security scheme

Proposed scheme ISRS has better results and able to detect the malicious nodes activities in the network. ISRS will help to secure the network where various types of malicious nodes disturb the data communication. The proposed security scheme is workable in high mobility of vehicle nodes, dynamic network topologies and unpredictable network [13-15].

V. Conclusion

Security is one of the significant concern for data communication for various safety applications in the network. In this paper, we have proposed an Intelligent Secure Routing Scheme (ISRS) to secure the data communication in VANETs. The proposed security scheme mainly focuses on malicious nodes and its false and wrong activities in the network. The proposed scheme selects a cluster head by signal strength and distrust value and higher value node will be selected as cluster head as a verifier. Road side units act as a certificate authority to help the CH in the network. In the case of any malicious node presence in the network, all vehicle nodes verifying the vehicle information from CH and if the information is wrong it will be added in the black list. Through extensive performance evaluation, we have demonstrated that ISRS has better results in term of data delay, throughput and detection ratio. In future, we will design complete security architecture for VANETs which has privacy concern as well.

References

[1] M. Sookhak, F. R. Yu, and H. Tang, "Secure Data Sharing for Vehicular Ad-hoc Networks Using Cloud Computing," in Ad Hoc Networks, ed: Springer, 2017, pp. 306-315.

[2] T. Qiu, N. Chen, K. Li, D. Qiao, and Z. Fu, "Heterogeneous ad hoc networks: Architectures, advances and challenges," Ad Hoc Networks, vol. 55, pp. 143-152, 2017.

[3] A. Vaibhav, D. Shukla, S. Das, S. Sahana, and P. Johri, "Security Challenges, Authentication, Application and Trust Models for Vehicular Ad Hoc Network-A Survey," I.J. Wireless and Microwave Technologies, 3, 36-48, 2017.

[4] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," IEEE communications magazine, vol. 46, 2008.

[5] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," IEEE Transactions on Vehicular Technology, vol. 61, pp. 86-96, 2012.

[6] N. K. Chaubey, "Security analysis of vehicular ad hoc networks (VANETs): a comprehensive study," International Journal of Security and Its Applications, vol. 10, pp. 261-274, 2016.

[7] Z. Wei, F. R. Yu, H. Tang, C. Liang, and Q. Yan, "Security Schemes in Vehicular Ad hoc Networks with

Cognitive Radios," arXiv preprint arXiv:1611.06905, 2016.

[8] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEE Transactions on vehicular Technology, vol. 59, pp. 1606-1617, 2010.

[9] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP—Sybil attacks detection in vehicular ad hoc networks," IEEE journal on selected areas in communications, vol. 29, pp. 582-594, 2011.

[10] I. Memon, "A secure and efficient communication scheme with authenticated key establishment protocol for road networks," Wireless Personal Communications, vol. 85, pp. 1167-1191, 2015.

[11] L. Wei and C. Zhang, "TrInc-based Secure and Privacy-preserving Protocols for Vehicular Ad Hoc Networks," in Vehicular Technology Conference (VTC Spring), 2016 IEEE 83rd, 2016, pp. 1-5.

[12] M. Wang, D. Liu, L. Zhu, Y. Xu, and F. Wang, "LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication," Computing, vol. 98, pp. 685-708, 2016.

[13] R. W. Anwar, M. Bakhtiari, A. Zainal, and K. N. Qureshi, "Security in Wireless sensor network: Approaches and Issues," Indonesian Journal of Electrical Engineering and Computer Science, vol. 15, pp. 584-590, 2015.

[14] K. N. Qureshi, A. H. Abdullah, and J. Lloret, "Road perception based geographical routing protocol for vehicular ad hoc networks," International Journal of Distributed Sensor Networks, vol. 12, p. 2617480, 2016.

[15] K. N. Qureshi, A. H. Abdullah, J. Lloret, and A. Altameem, "Road-aware routing strategies for vehicular ad hoc networks: Characteristics and comparisons," International Journal of Distributed Sensor Networks, vol. 12, p. 1605734, 2016.