A New Security Approach for the Spectrum Access in Vehicular Networks

Ayoub Alsarhan
Dept. of Computer Information System
Hashemite University
Zarqa, Jordan
e-mail: ayoubm@hu.edu.jo

Ahmed Al-Dubai
School of Computing
Edinburgh Napier University
Edinburgh, UK
e-mail: a.al-dubai@napier.ac.uk

Yousef Kilani
Dept. of Computer Information System
Hashemite University
Zarqa, Jordan
e-mail: ymkilani@hu.edu.jo

Muhsen Alkhalidy
Dept. of Computer Science and Applications
Hashemite University
Zarqa, Jordan
e-mail: muhsen@hu.edu.jo

***Abstract*— Vehicular ad hoc networks (VANETs) have been instrumental in intelligent transportation systems that enhances road safety and road management significantly. This technology enables communication among vehicles where drivers can share road information conditions. However, users can threaten spectrum access caused by launching passive and active attacks that prevent nodes to access spectrum efficiently. Securing spectrum access has become critical issue in VANET to ensure reliability and trustworthiness. In this paper, a novel collaborative approach during the spectrum access process is proposed. In our approach, vehicles are divided into clusters and Road Side Unit (RSU) is used to manage spectrum access for each cluster. RSU monitors the traffic for each node and identifies the malicious and misbehaving nodes. The proposed approach measures the node's data reliability using a decision function. The scheme is applicable to a wide range of VANET applications, such as traffic safety, commercial applications, and Internet access.**

Keywords— Resource management; VANETs; trust management; security; misbehavior detection.

I. INTRODUCTION

Recently, VANETs are adopted to enhance road safety and to improve efficiency of traffic management. In VANET, vehicles cooperate to relay warning messages and road condition which improve safety significantly [1]-[3]. Each node in VANET (i.e., vehicles and RSUs) are equipped with different environmental sensors, processing, and wireless communication devices. VANETs support various applications that have been developed to innovate solutions to real life problems [1]-[3]. These applications include life safety, commercial applications, and Internet access. VANETs' applications can be classified based on communication model into the following categories: Vehicle to Infrastructure (V2I), Vehicle to Vehicle (V2V) and the hybrid communication.

In order to enhance road safety, vehicles should monitor the nearby vehicles to avoid accidents. Traffic status might be stored at RSU where collected data from vehicles can be processed and then RSU disseminates road status to other vehicles. Because vehicles move at high speeds, the likelihood of VANET disconnection increases. Thus, sufficient number of road side units should be installed to maintain connectivity in VANET. Some of VANETs' applications, i.e., safety applications, require timely and accurate data. However, VANETs are vulnerable to numerous security threats and attacks that may make VANETs unavailable to the users. These attacks have several impacts on the VANET performance and users. For instance, the following are attacks that VANET may face [4]:

- Attacker may send false messages about the road status. The attacker may send wrong information in VANETs to vehicles for exchanging this information.
- The misbehaved vehicle may change the context of messages over VANET.
- The malicious vehicle sends a high volume of messages to overwhelm nodes, reserve VANETs' bandwidth, and consume nodes' resources.
- The eavesdropper vehicle injects some malicious codes to crash the control system in vehicle.

In safety application, any vehicle in VANET detects an accident, emergency or sudden changes in speed or direction should report new road status to RSU [1]-[3]. RSU disseminates traffic alerts to all vehicles in the cluster. Warning messages should be delivered very fast in a high reliable manner to prevent accidents. However, if the reported data to RSU is faulty or malicious, then a traffic jam can take place, thus, result in life-threatening [4]. Hence, it is necessary to secure data communication in VANETs. The rest of this article is organized as follows. First, related work and our contributions to the paper are introduced in Section II. Next, VANET is presented in Section III. We describe the proposed security scheme in Section IV. Then, we present some of the performed tests and show the performance of the VAET under different conditions with our scheme in Section V. Finally, the article is concluded in Section VI.

II. BACKROUND

Recently, there has been growing research interest and a great deal of emphasis placed in VANET security. In [5], authors proposed a new security scheme where public key infrastructure is used for message authentication and integrity. Large number of anonymous public/private key

 ISBN: 978-1-61208-685-9

pairs and the corresponding public key certificates are stored in each vehicle. A public/private key pair are used by each vehicle to avoid movement tracking. However, each node would require very high storage capacity to save many key pairs and corresponding certificates. Furthermore, each node should store all anonymous certificates of vehicles. Hence, message verification incurs high cost using this scheme.

In [6], authors proposed CARAVAN scheme where vehicles are divided into groups and the leader for each group acts as a proxy on behalf of all group members. Authors in [7] proposed new Cooperative Neighbor Position Verification (CNPV) security scheme. CNPV uses several heuristics for messages verification. These heuristics include direct verification, crosschecking, and multipoint location verification. CNPV detects any node announcing false positions and this node is prevented from relaying any message in the network. CNPV considers only nodes that advertise correct information about their positions to forward critical information. It adopts support vector machine (SVM) classifier to determine the authenticity of the messages. SVM uses vehicle attributes and message content for detecting untrustworthy nodes.

In [8], the proposed scheme determines the false messages by monitoring the behavior of nodes after receiving the road status reports. It computes the "degree of belief" for each primary information by correlating secondary information observed by more than one node. Authors proposed new filter in [9] to specify spurious messages. Messages should pass through two-layer filter for classification purposes. In the first layer, some features for the message are used for rapid filtration. These features include digital signature verification, time validation, geographic location validation, and support from RSU. In the second phase, alert message is evaluated accurately. The filter uses incremental back propagation neural network (BPNN) and the support from neighbors to recognize the behavior the node. Authors in [10] proposed a new scheme for intrusion detection that combines BPNN and support victor machine for spurious messages.

Some security schemes adopt node reputation for detecting untrustworthy nodes. Reputation is approximation of node behavior based on collective opinion about a node [11]. It represents node's behavioral history which is used to predict node behavior in future. In [11], authors proposed new reputation management approaches. To detect hackers/liars, they suggested new service reputation and feedback reputations. The proposed scheme integrates trust management model with a pseudonym technique to preserve privacy. Reputation model is used to resist the tactical attacks. In order to recognize false messages, information entropy and majority rule are integrated to reputation algorithm. In [12], distributed trust model (DTM) is proposed for motivating selfish nodes to cooperate more. For each node, the cost for sending data is computed based on the node's behavior, so that malicious nodes pay more for communication. Most of the existing security schemes for VANET focus only on assessing the trustworthiness of nodes by analyzing the history of the nodes. However, these schemes have omitted the evaluation of the trustworthiness of the data shared among these nodes in VANET. In contrast, our scheme detects malicious nodes based on reported data. These nodes are evicted form VANET by RSU. Thus, multiple attacks can be avoided by focusing on nodes' data instead of focusing on the attacks. In order to improve the accuracy of trust function, the trust level for each node is calculated considering the trustworthiness of data. Moreover, the trust model makes a decision more scientifically, dynamically, and adaptively where trust level for each node is calculated and changed with the number of communication interactions.

Figure 1. Architecture of VANET

III. NETWORK OVERVIEW

Each road is divided into K segments. We assume that the existence of RSU manages the traffic at each segment (cluster). Each node is equipped with a single IEEE 802.11b based transceiver. The spectrum is partitioned into non-overlapping channels (16 channels for each RSU with 5 MHZ spacing with transmission and power mask restrictions similar to the ISM band), which is the basic unit of allocation.

Our system model for VANET is depicted in Figure 1 where both communications model are allowed (i.e., V2I, and V2V). Each vehicle is outfitted with radio communication gear that acts as a relay point for other nodes as well as an RSU. In our work, all vehicles are equipped with assistance of on-board sensors. These sensors include an GPS receiver, speedometer, accelerometer, and digital map to help a vehicle to gather road data. Each node in the cluster senses the road status and reports the data to RSU. Each vehicle is considered within the range of i^{th} RSU if:

$$S_{j,i} \geq T \tag{1}$$

where $S_{j,i}$ is the signal power received at i^{th} RSU from j^{th} node, and T is the threshold for signal power. Signal power is computed as follows:

$$S_{j,i} = S_0 (\frac{d}{d_0})^{-n} \tag{2}$$

where d_0 is the close-in reference distance, n is the path loss exponent, and S_0 is the signal power at distance d_0.

 ISBN: 978-1-61208-685-9

IV. PROPOSED APROACH

Each vehicle in VANET gets a value called a trust level (T_l), which describes the level of reliability of the node. Trust level for a node is computed as follows:

$$T_l = \frac{F_m}{T_m} \tag{3}$$

where F_m is the number of false messages that a node sent, and T_m is the total number of messages that were sent by a node. Trust level (T_l) is the key parameter in our scheme to secure VANET by monitoring the nodes' activities and detect the misbehaving nodes. Our scheme handles four different behavior categories (ways) that may threaten VANET and degrades its security and performance. The following threat model is considered in this paper:

(i) Selfish behavior where a node does not follow VANET's protocol. An attacker does not cooperate with nodes in VANET and rejects to forward data packets.
(ii) A node behaves in a malicious, misbehaving, and cheating way where it emulates RSU and sends false status of road to other nodes in VANET.
(iii) A node behaves in a malicious, a node launches denial of service (DoS) attack one or more VANT's resources (i.e., medium, and RSU) to prevent other nodes from accessing VANET for their data transmission.
(iv) One or multiple adversary nodes may launch objective function attack to change communication parameters such as signal power, center frequency, encryption type, and public-key cryptography and the symmetric key cryptography.

The main objectives of our scheme are threefold, namely *high data rate*, *secure communication* and *maximizing VANET utilization*. To make the communication in VANET secure, the public-key cryptography and the symmetric key cryptography are generated and used for communication between nodes. Firstly, public-key cryptography is used in VANET to ensure data security until a symmetric key is shared between RSU, and the node. The symmetric key is generated and assigned to new node in the class during the node's authentication process. It is worth indicating that the key is used for encrypting and decrypting all messages in VANET.

A symmetric key is used to encode the messages. The receiver decodes the data using the same key. Nodes exchange certificates, IDs, and symmetric key. RSU keeps track of all nodes in its cluster. After gathering road data, all nodes send their data to RSU. The data gathered by node j are represented by vector Xj . For node j , RSU compares the node's j data with other nodes and if they match, RSU decides that node j is a trustworthy node; otherwise it is untrustworthy node. The dissimilarity between node's j data and node i is computed as follows:

$$d_s(i,j) = \max_f \left| X_i(f) - X_j(f) \right| \tag{4}$$

where $X_i(f)$ is the f^{th} dimension for j^{th} node. Each dimension of the vector X_i corresponds to an attribute of a vehicle. Each node constructs more than one vectors which contain information about vehicles in the road. The vector includes the speed of each vehicle on the cluster, and the position for the vehicle. Each node gathers information and sends the data periodically to RSU through beacon messages. Upon the reception of the different data reports from the cluster nodes, RSU analyzes these reports to extract the road status and decides the reliability of the reported nodes. A decision functions a bout j^{th} node can be described using the following function:

$$Q_j = \begin{Bmatrix} 1, d_s(i,j) \geq \gamma, \forall j \in G \\ 0, d_s(i,j) \prec \gamma, \forall j \in G \end{Bmatrix} \tag{5}$$

where G is the set of nodes in VANET, and γ is the dissimilarity threshold. Q_j is a decision function that is executed by a RSU to decide whether j^{th} node is trustworthy or not. RSU decides whether the j^{th} node is untrustworthy if the dissimilarity between node's j data and node i is greater than threshold γ . RSU selects node based on the trust level. RSU does not receive data from untrustworthy nodes. It informs other nodes in VANET to discard any message from these nodes. Therefore, spectrum utilization is increased significantly.

V. PERFORMANCE EVALUATION

We simulate the proposed scheme to specify the adversary nodes in VANET which degrade the performance of the network. Table I shows the network simulated with values used for the parameters required. Results are analyzed to clarify the importance and the effectiveness of our scheme to secure data over VANET by monitoring nodes behavior and analyzing nodes' data. The key performance measures of interest in the simulations are:

(1) Throughput, which is the average rate of successful message delivery over a communication channel.
(2) Utilization, the average amount of time the spectrum is kept busy. The utilization is calculated as follows:

$$U = \frac{B_t}{S_t} \tag{6}$$

where B_t is the amount of time in which the spectrum is kept busy, and S_t is the simulation time. The results are averaged

 ISBN: 978-1-61208-685-9

over enough independent runs so that the confidence level is 95% and the relative errors do not exceed 5%. We examine the performance under different parameter settings.

TABLE I. SIMULATION PARAMETERS

Parameter		Value
Number of nodes		200
Number of channels per RSU		40
Number of messages per node		Random
Type of interface per node		802.11 b
MAC layer		IEEE 802.11 b
Transmission power		0.1 watt
Packet size		512
Max Vehicle Speed		80 km/h
Number of malicious nodes		10,20,30,40, 50
Simulation Device	Intel i5 Core	2.50GHz
	Process cores	2 x 2.50GHz
	RAM	6 GB
	OS	Windows 7 64 bit

Figure 2 illustrates the simulation results in terms of throughput for VANET using our security scheme (secure VANETs, (SV)) and VANET without security mechanism (NSV). It is apparent that from the figure that the throughput shifts into higher level when the number of malicious nodes decreases to the lowest possible number. Sometimes, malicious nodes reject forwarding packets. Furthermore, the attacker might keep sending RSU false reports to gain exclusive access to the spectrum and to prevent other nodes from utilizing unused spectrum. Hence, the number of dropped packets increases significantly, which lowers throughput. Packet drop ratio is plotted under various number of malicious nodes as shown in Figure 3. It can be observed that the drop ratio increases as the number of malicious nodes is increased. Our scheme excludes malicious nodes in VANET. Thus, drop ratio is decreased when attack is detected and attackers are prevented from forwarding packets.

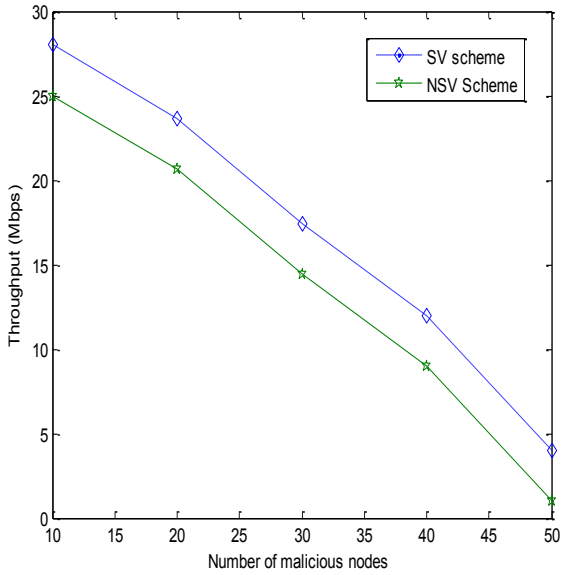

Figure 2. Throughput comparison for the two schemes

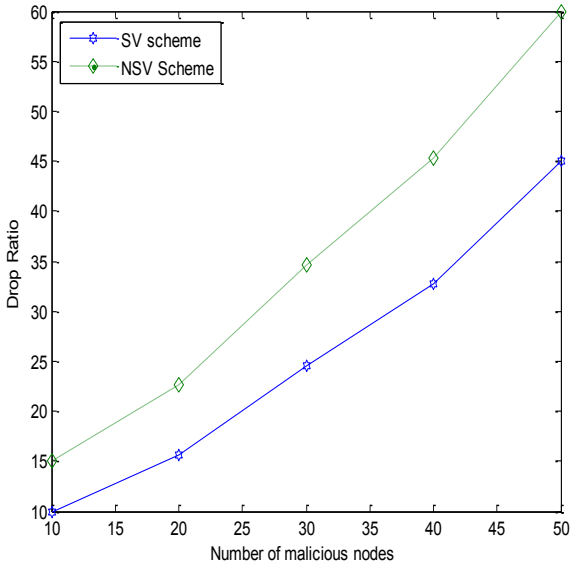

Figure 3. Packet drop ration comparison for the two schemes

For fixed arrival rate, the utilization for VANET's resources is plotted under various number of malicious nodes in Fig. 4. It can be observed that system utilization decreases as the number of malicious nodes is increased. Dummy messages are sent by attackers to jam channels and reserve VANETs' resources. Hence, VANET will not be available to licensed users. The results in Fig. 4 show the ability of our scheme to enhance the utilization of the network's resources. In our scheme, RSU does not receive reports from untrusted nodes. Furthermore, it informs trustworthy to neglect untrusted nodes' messages. Thus, untrusted nodes are prevented from forwarding messages and they won't be able to generate false messages to RSU.

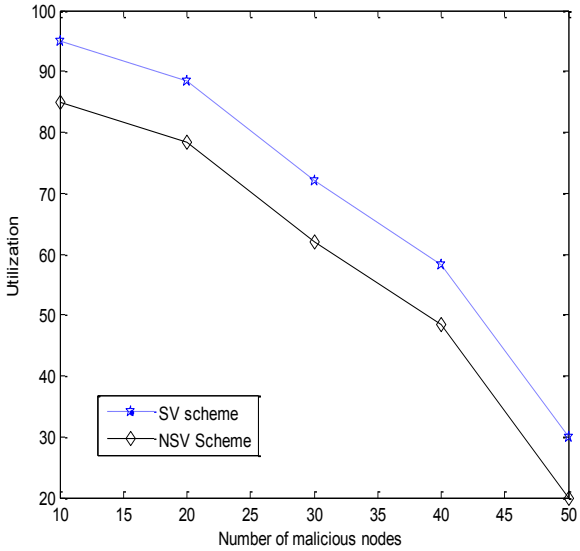

Figure 4. Utilization comparison for the two schemes

 ISBN: 978-1-61208-685-9

VI. CONCLUSION AND FUTURE WORK

Securing VANET communication is very important to save lives by guiding drivers to spotting hazards and improving road safety and traffic conditions. Different attacks might be launched by adversary nodes. These attacks degrade the performance and reliability of VANET significantly. Thus, this paper has presented a security scheme that monitors nodes behavior in VANET to identify and to exclude adversary nodes. In this paper, the trustworthiness of data is evaluated for each node to extract the set of untrustworthy nodes. To validate the proposed scheme, we conducted simulation experiments. The experimental results stress the ability of our scheme to improve the performance of VANET by eliminating malicious nodes. As future directions, several criteria will be used to assist the node trust, including, functional trust and recommendation trust from other nodes. In addition, different operating scenarios and conductions will be considered.

REFERENCES

[1] S. K. Bhoi and P. M. Khilar, "Vehicular Communication - A Survey," *IET Networks*, vol. 3, no. 3, pp. 204-217, 2014.

[2] S. Bitam, A. Mellouk and S. Zeadally, "VANET-Cloud: A Generic Cloud Computing Model for Vehicular Ad Hoc Networks," *IEEE Wireless Communications*, vol. 22, no. 1, pp. 96-102, February, 2015.

[3] T. W. Chim, S. M. Yiu, L. C. K. Hui and V. O. K. Li, "VSPN VANETBased Secure and Privacy-Preserving Navigation," *IEEE Trans. On Computers*, vol. 63, no. 2, pp. 510-524, February, 2014.

[4] Hasrouny, H., Samhat, A.E., Bassil, C. and Laouiti, A., VANet security challenges and solutions: A survey, *Vehicular Communications*, 7, pp.7-20., 2017

[5] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security – Special Issue Security Ad Hoc Sensor Networks*, vol. 15, no. 1, pp. 39-68, 2007.

[6] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura and K. Sezaki, CARAVAN: providing location privacy for VANET, in: *Proceedings of the Workshop on Embedded Security in Cars (escar)'05*, 2005.

[7] M. Fogue *et al*., "Securing Warning Message Dissemination in VANETs Using Cooperative Neighbor Position Verification," in *IEEE Transactions on Vehicular Technology*, vol. 64, no. 6, pp. 2538-2550, June 2015.

[8] A. Vulimiri, A, Gupta, Pramit Roy, S Muthaiah and A. Kherani "Application of secondary information for misbehavior detection in VANETs," in Proc. NETWORKING 2010, Chennai, India, pp. 385-396, 2010.

[9] J. Zhang, L. Huang, H. Xu, M. Xiao and W. Guo, "An Incremental BP Neural Network Based Spurious Message Filter for VANET," *2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, Sanya, pp. 360-367, 2012.

[10] Y. Liu, Y. Shi, H Feng, and L. Wang, "Intrusion detection scheme based on neural network in vehicle network," *J. Communs*., vol. 35, no. Z2, pp. 32-239, Nov. 2014.

[11] J. Wang, Y. Zhang, Y. Wang, and X. Gu, "RPRep: A robust and privacy-preserving reputation management scheme for pseudonym-enabled VANETs," *Int. Journal Distributed. Sensor Network*, vol. 2016 , Art. no. 6138251, 2016

[12] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "A job market signaling scheme for incentive and trust management in vehicular ad hoc networks," *IEEE Trans. Vehicular Technology*, vol. 64, no. 8, pp. 3657-3674, Aug. 2015.

 ISBN: 978-1-61208-685-9