Trust-based Model for Securing Vehicular Networks Against RSU Attacks

Aljawharah Alnasser
Department of Information Technology
King Saud University, Riyadh, Saudi Arabia

Hongjian Sun
Department of Engineering
Durham University, Durham, UK

***Abstract*—Intelligent Transportation System (ITS) is one of the Internet of Things (IoT) systems that can achieve reliable transportation by providing communications between vehicles and infrastructure units. The interaction between them is called Vehicle-to-Everything (V2X) communication that is bridged by LTE-V2X protocol. However, a V2X communication link faces a significant challenge in cyber-security. Road entities and Road Side Units (RSUs) are exposed to various cyber-attacks, including internal and external attacks. Internal attackers have valid credentials; thus, detecting them is still a challenge. As a result, a trust model was suggested by existing work to protect the network against internal attackers. In this paper, a global trust-based model is proposed for securing V2X communications against RSU attacks. Trust decision is made based on two levels: distributed and global levels. Each road entity can make its local decision based on the distributed trust model. Additionally, the central server has the responsibility to make the global decision and reduce the impact of various RSU attacks. Also, multiple experiments are conducted with different percentage of malicious RSUs to measure the performance of the proposed model. Simulation results show that the proposed model achieves lowest Packet Dropping Rate (PDR) values for various number of malicious nodes in comparison with existing models.**

***Index Terms*—Trust, V2X, RSU attacks.**

I. Introduction

The evolution of computer networks leads to the creation of a new form of communication between smart objects known as the Internet of Things (IoT). IoT transforms all solid objects to smart ones by embedding extra hardware to be able to sense, communicate, and make decisions. It changes the traditional transportation system by improving the capabilities of all road entities such as vehicles, cycles, and motorcycles to form the Intelligent Transportation System (ITS). The communication between road entities and Road Side Units (RSUs) is called Vehicle-to-Everything (V2X), which can be supported by LTE-A (e.g, release 14).

As a consequence, the road entity and RSU are vulnerable to internal and external attacks. Internal attackers could disrupt the network performance without being detected as they are authenticated nodes. Thus, trust management was proposed to monitor the nodes' behaviour. When misbehaviour is detected, the misbehaving node could be classified as an internal attacker.

Existing research in the vehicular network assumes that the RSU is a trusted node where all trust calculations are done on these nodes. For instance, Sedjelmaci and Senouci [1] proposed a framework as an intrusion detection system that focused on behavioural attacks in Vehicular Ad-hoc Networks (VANETs). Predefined agents are responsible for monitoring the nodes' behaviour and broadcasting an alarm when the misbehaviour is detected. The framework is composed of a node detection system, a cluster detection system and a global decision system. The first detection system is implemented on each node to monitor its surrounding nodes. The second detection system runs at the cluster head level. Finally, global decision system runs at RSU level to calculate the trust level for each node and broadcast the blacklist through the network. Also, the proposed framework in [2] implemented various security checks to measure the message's trustworthiness. It computes the trust value for each road section and each neighbourhood. Once the message is evaluated and considered trusted, then it looks up for a trusted route to forward the message. In addition, Kerrache *et al.* [3] implemented a trust model that provided two trust metrics: vehicle-based and RSU-based. Each node can monitor its neighbours and compute local trust value. Then, RSUs are responsible for maintaining global and past trust information about all nodes which reside in the same road segment.

Traditional security models used RSU as a part of the security process. For example, Lei *et al.* [4] introduced a novel key management scheme for key exchange among security managers in heterogeneous networks. They used the blockchain concept for secure key exchange within the network. The flexible transaction collection period was proposed to decrease the key exchange time in the blockchain scheme. The work of [5] implemented a model that achieved privacy and non-repudiation requirements. It consists of two schemes which are identity-based signature and pseudonym. Also, it provides authentication in inter-vehicle communications. Also, Zhang in [6] proposed a novel method based on one-time identity-based authenticated asymmetric group key agreement to create cryptographic mix-zones which resists

978-1-7281-1025-7/19/$31.00

malicious eavesdroppers. The safety messages are encrypted using a group secret key to improve vehicles' privacy. Thus, an external entity cannot track the safety messages in the cryptographic mix-zones.

However, this is not applicable where RSUs also are vulnerable to malicious attacks. Indeed, Hamida *et al.* [7] mentioned that RSUs are not fully trusted nodes. In addition, based on [8] [9], the RSU could be considered as a normal or malicious terminal. As a result, in the case of RSU attacks, existing solutions will not work efficiently, and then they worsen the network performance. For instance, Hao *et al.* [10] developed security protocols for the key distribution, that can detect the compromised RSUs and their cooperation with the malicious vehicles. However, the model protects the network only against external attackers.

As a consequence of ignoring the malicious behavior of RSUs, the trust model could make inaccurate decisions. Therefore, this paper proposes a trust-based model that is able to detect malicious RSUs and road entities. When the entity is connected with the core network, it receives the updated global blacklist. The central server has the responsibility to make the global decision and reduce the impact of various RSU attacks. The performance of the proposed model is evaluated by comparing it with existing models [11], [12]. The simulation results show that the proposed model outperforms the existing models [11], [12]. This paper makes three main contributions to the field of vehicular networks' security:

- Different from existing research, this paper proposes a global trust-based model for V2X communications with protection against RSU attacks. A new algorithm for decision computation regarding RSUs is proposed for the first time.
- The improvement of the trust decision is studied when applying the global decision system in comparison with the distributed model in [11].
- This paper compares the performance of the proposed model with the existing models in [11], [12]; the proposed model achieves lowest Packet Dropping Rate (PDR) values for various percentage of malicious nodes in comparison with existing models. Also, it provides excellent improvement in FNR values, which is around 74% in comparison with the model in [11].

The remaining of this paper is organised as follows. Section II presents the system model. Section III provides a detailed description of the proposed trust model. Section IV includes both simulation set-up and experimental results. Section V focuses on performance comparison with the existing model [11], [12]. Section VI draws conclusions.

II. System Model

The considered network is a vehicular network which is composed of N road entities including vehicles, cycles, motorcycles, and pedestrians, and M' fixed RSUs. The road entities move at various speeds through a dedicated route. Each time the road entity sends a message to the core network, it should first examine its connectivity with the core network and the surrounding entities. Then, if the source entity has a connection with the core network, it forwards its packet to the nearest RSU. Otherwise, the packet is sent to a trusted road entity to relay it to the core network.

Moreover, the network has two types of entities which are normal and malicious. The normal entity includes normal road entities and RSUs. The normal road entity monitors the surrounding entities, sends and relays packets to the core network. In addition, the road entity can measure the trustworthiness of the neighbouring entities. In addition, the malicious road entities launch various attacks to disturb the network performance such as:

- Selective forwarding attack: occurs when the malicious road entity drops some of the received packets randomly to escape punishment.
- Recommendation attack: occurs when the malicious road entity sends bogus recommendations regarding other entities.
- On-off attack: occurs when the malicious road entity behaves normally and maliciously alternately with time.

Moreover, normal RSUs keep receiving warning messages from road entities and make decisions based on the volume of warning messages. Then, it sends its decision to the central server. On the other hand, the malicious RSU initiates recommendation attacks to disturb the trust decision by sending malicious warnings to the central unit regarding normal nodes or dropping the malicious warnings regarding other malicious nodes.

III. Trust-based Model for securing against RSU attacks

The trust-based model manages two levels of trust [13]: *distributed level* and *global level*. At distributed level, the road entity measures the trustworthiness of neighbouring entities; then, it sends warning messages to the surrounding RSUs in case of detecting malicious behaviour. At global level, when the RSUs received high volume of warning messages regarding a misbehaviour road entity, they will send an alarm to the central unit. Then, the central unit can make global decision based on the number of alarm messages. All road entities are able to apply distributed trust model. Beside distributed model, when the road entity is connected to one or more RSUs, it can apply the global trust model. The details about the proposed model are presented as follows.

A. Distributed trust model

Each time interval t, the road entity computes the local trust of all neighboring entities. Indeed, node i continuously

monitors and collects information regarding its one-hop neighbours j. Then, node i can measure direct trust using the collected information. In addition, node i sends recommendation requests to the surrounding nodes k regarding node j. The proposed model maintains three trust components and local decision as follows.

- **Direct Trust -** $T^{(t)}_{direct(i,j)}$: it is computed by node i to assess the direct connection with node j during time interval t. It is measured by

$$T^{(t)}_{direct(i,j)} = \frac{T^{(t)}_{past(i,j)} + T^{(t)}_{current(i,j)}}{2} \tag{1}$$

  It is measured based on the following trust values:

  - *Past trust* - $T^{(t)}_{past(i,j)}$: it is an evaluation for the historical behaviour of node j. Past trust is considered to reduce the impact of on-off malicious attacks. It is calculated by

$$T^{(t)}_{past(i,j)} = T^{(t-\Delta)}_{l(i,j)} \tag{2}$$

    where $T_{l(i,j)}$ is the recorded local trust value in the previous trust interval $(t-\Delta)$. Δ is the time duration from the last computed trust value for node j.
  - *Current trust* - $T^{(t)}_{current(i,j)}$: it is an assessment for the quality of direct communications with neighbouring nodes j. It is computed using

$$T^{(t)}_{current(i,j)} = \frac{SI^{(t-\Delta)}}{TI^{(t-\Delta)}} \tag{3}$$

    where $SI^{(t-\Delta)}$ is the number of successful interactions between node i and node j since the last trust interval, and $TI^{(t-\Delta)}$ is the total number of interactions between node i and node j since the last trust interval.

- **Indirect Trust -** $T^{(t)}_{indirect(i,j)}$: it is a measure for the behaviour of neighbouring nodes j by considering the surrounding nodes' opinions. Node i collects recommendations from the neighbouring nodes k regarding node j. The confidence value $C^{(t)}_{(i,k)}$ is computed for each recommender node k to minimize the impact of recommendation attacks. it is computed by

$$C^{(t)}_{(i,k)} = \begin{cases} 1, & \text{if } T^{(t)}_{l(i,k)} \geq Th_{max}. \\ C_w, & \text{if } Th_{min} \leq T^{(t)}_{l(i,k)} < Th_{max}. \\ 0, & \text{if } T^{(t)}_{l(i,k)} < Th_{min}. \end{cases} \tag{4}$$

  where C_w is the confidence weight for uncertain recommendations. After that, each node i calculates indirect trust for node j using

$$T^{(t)}_{indirect(i,j)} = \frac{\sum_{k=1}^{\alpha}[C^{(t)}_{(i,k)} \times T^{(t)}_{l(k,j)}]}{\alpha} \tag{5}$$

  where α is the number of received recommendations about node j.

- **Local Trust -** $T^{(t)}_{l(i,j)}$: each node i can calculate local trust for node j and make a local decision. Generally, the local trust value is computed using Table I. It is changed based on three factors which are the existence of current communications between node i and node j; the existence of the recommendations regarding node j; and the presence of a previous connection between node i and node j. w_1 and w_2 are weights for indirect trust and (direct/current or past) trust respectively. w_1 represents the recommendation rate as follows:

$$w_1 = (m+n) \times \frac{RC}{Neighbors^{(t)}} \tag{6}$$

  where $w_2 = 1 - w_1$, RC is the recommendation factor, and $Neighbors^{(t)}$ is the number of node i neighbors at time t.

- **Local decision**: node i has a local blacklist which has a list of malicious nodes based on the local decision. Thus, node i stops the communication with any node j in the blacklist. The decision is made using

$$D_{Local} = \begin{cases} Trusted, & \text{if } T^{(t)}_{l(i,j)} \geq Th_{max}. \\ Uncertain, & \text{if } Th_{min} \leq T^{(t)}_{l(i,j)} < Th_{max}. \\ Malicious, & \text{if } T^{(t)}_{l(i,j)} < Th_{min}. \end{cases} \tag{7}$$

  where Th_{min} and Th_{max} are minimum and maximum trust thresholds, respectively. After that, the node updates its local blacklist and sends malicious and uncertain warning messages to the surrounding RSUs.

B. Global Trust model

During time interval t', where $t' > t$, RSUs start trust calculation phase. First, each RSU measures the percentage of malicious and uncertain alarms regarding node j using

$$M_{(j)} = \frac{m_j}{t'}, \qquad U_{(j)} = \frac{u_j}{t'} \tag{8}$$

where m_j and u_j are the number of malicious and uncertain warnings regarding node j respectively. Second, each RSU is able to make a decision regarding node j using

$$Decision_{(RSU,j)} = Rate_{M(j)} - Rate_{U(j)} \tag{9}$$

where $Rate_{M(j)}$ and $Rate_{U(j)}$ are the rates of malicious alarms and uncertain alarms respectively. They are calculated using

$$Rate_{M(j)} = \frac{M_{(j)}}{TM_{(j)}} \tag{10}$$

where $TM_{(j)} = M_{(j)} + U_{(j)}$ and $Rate_{U(j)} = 1 - Rate_{M(j)}$. Finally, the RSU applies Algorithm 1 to make a decision regarding node j. Therefore, if node j is classified as

TABLE I
LOCAL TRUST COMPUTATION

Has current communication	Has recommendations	First time communication	Has previous communications
Y	Y	$T^{(t)}_{l(i,j)} = w_1 \times T_{indirect(i,j)} + w_2 \times T_{current(i,j)}$	$T^{(t)}_{l(i,j)} = w_1 \times T_{indirect(i,j)} + w_2 \times T_{direct(i,j)}$
Y	N	$T^{(t)}_{l(i,j)} = T_{current(i,j)}$	$T^{(t)}_{l(i,j)} = T_{direct(i,j)}$
N	Y	$T^{(t)}_{l(i,j)} = T_{indirect(i,j)}$	$T^{(t)}_{l(i,j)} = w_1 \times T_{indirect(i,j)} + w_2 \times T_{past(i,j)}$
N	N	$T^{(t)}_{l(i,j)} = T^{(0)}_{l(i,j)}$	$T^{(t)}_{l(i,j)} = T_{past(i,j)}$

Input: $R \leftarrow$ list of RSUs, $N \leftarrow$ list of road entities, $Th_R \leftarrow$ RSU threshold.

for each RSU R(L) **do**
  for each $R(L).warningList_j$ **do**
    $w \leftarrow R(L).warningList_j(index)$
    if $w.NotDuplicated()$ **then**
      if $w.isMalicious$ **then**
        $m_j \leftarrow m_j + 1$
      else
        $u_j \leftarrow u_j + 1$
      end if
    end if
  end for
  for each node $N(l)$ **do**
    $Decision_{(R(L),N(l))} \leftarrow \frac{M_{N(l)} - U_{N(l)}}{M_{N(l)} + U_{N(l)}}$
    if $Decision_{(R(L),N(l))} > Th_R$ **then**
      $Send\ alarm\ to\ the\ central\ server$
    end if
  end for
end for

Algorithm 1: Algorithm for decision computation on RSU level

malicious node, the RSU sends malicious alarm to the central server.

At this stage, the central server can make global decision regarding node j based on the alarms which are received from RSUs.

$$D_{Global} = \begin{cases} Malicious, & A_m > Th_G. \\ Normal, & A_m \leq Th_G. \end{cases} \tag{11}$$

where A_m is the number of malicious warnings that are received regarding node j and Th_G is the global trust threshold. Node j is added to the global blacklist when it is classified as a malicious node. Then, the central server broadcasts the updated global blacklist to RSUs. Then, RSUs rebroadcast it again to all roads entities that are covered by the network. The road entities update their local blacklist based on the received global blacklist.

IV. SIMULATION ANALYSIS

This section explains the simulation set-up for evaluating the performance of the proposed model. The effect of changing parameters on the false alarm rate is analysed. Also, we study the impact of RSU attacks on False Negative Rate (FNR), False Positive Rate (FPR), and PDR.

A. Network specifications

We used MATLAB R2016b to conduct the simulation of a V2X network with 24 road entities and 9 RSUs with parameters, as shown in Table II. The road entities move over an area of $800 \times 800\ m^2$ with various speed ranges. The road entity sends the transaction message to the core network directly or using a multi-hop routing protocol. To measure the performance of the proposed trust model, we study various types of malicious road entities and RSUs.

B. Experiment results

1) Study of the impact of Global decision threshold (Th_G) on false alarm rate: The impact of various values of the global threshold on the false alarm rate is studied. The global threshold is between 1 and 9, which represent the number of RSUs in the network. As shown in Table III, the FNR increases when the threshold increases because the node is classified as a malicious node when the number of malicious warning is greater than the global threshold.

TABLE II
SIMULATION PARAMETERS

Parameter	Value
Simulation time	600 iteration
Speed ranges	Vehicle:(10-30) m/s, Pedestrians:(0-8) m/s Cycles:(3-10) m/s, Motorcycle:(10-30) m/s
RSU's communication range	100 m
Road entity communication range	200 m
Th_{max}	0.7
Th_{min}	0.4
Th_G	3
Th_R	0
RC	0.3
C_w	0.9
$T^{(0)}_{l(i,j)}$	0.5

TABLE III
FNR AND FPR FOR VARIOUS VALUES OF Th_G

Global decision threshold (Th_G)	FNR	FPR
1	0.0212	0.0638
2	0.0216	0.0638
3	**0.0219**	**0.0638**
4	0.0258	0.0638
5	0.0535	0.0638
6	0.0535	0.0638
7	0.0860	0
8	0.0860	0
9	0.0860	0

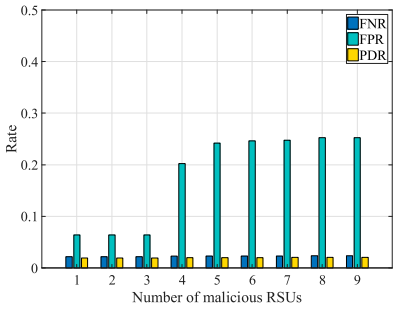
Therefore, the central server should receive nine malicious warnings in case the threshold is equal to 9. On the other hand, FPR is stable until the threshold becomes greater than or equal to 7. The FPR is equal to zero with high values of thresholds because the honesty of the received malicious warning is ensured. As a result, the effect of the bad-mouthing attack is controlled. The choosing of optimal value should consider the balance between FNR and FPR values. Thus, $Th_G = 3$ is the optimal value which achieves low FNR and fair value of FPR.

2) Study of the impact of various RSU attacks: The experiments are conducted to study the impact of malicious behaviour of RSUs on various metrics, which are FNR, FPR, and PDR. In this study, the bad-mouthing attackers send fake recommendations regarding four normal road entities.

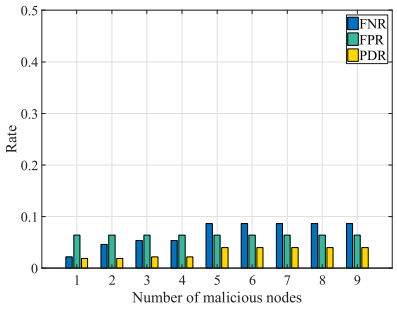
- Bad-mouthing attacks: The impact of the various number of malicious RSUs, which launch the bad-mouthing attack, on the proposed metrics is studied. As shown in Fig. 1 (a), the FPR values goes up when the number of malicious RSUs increases. The increasing starts at the fourth RSU. On the other hand, the FNR and PDR are not affected and remains stable for the various number of malicious RSUs.
- Good-mouthing attacks: The impact of the various number of malicious RSUs, which launch the good-mouthing attack, on the proposed metrics is examined. In Fig. 1 (b), the FNR value increases when the number of malicious RSUs goes up. As a result of incorrect decisions regarding malicious node, the PDR value increases. On the other hand, the FPR is not affected and remains stable for the various number of malicious RSUs.

V. PERFORMANCE EVALUATION

We use trust-based trust models in [11], [12] to evaluate the performance of the proposed model. The model in [11] is the previous version of the proposed model which is based on distributed structure. The model in [12] considered two trust components which are direct and indirect to filter out bogus recommendations. Both existing models are



(a) Bad-mouthing attack



(b) Good-mouthing attack

Fig. 1. Effect of RSUs attacks on FNR, FPR and PDR: a) Bad-mouthing attack; b) Good-mouthing attack

distributed and they lack of a global knowledge regarding the malicious entities.

A. Study of the improvement in Trust model with a global decision system

An experiment is conducted to study the improvement rate in the global decision system. The local blacklist is evaluated on each node at the end of the simulation, and the rate of non-detected malicious nodes is measured. Also, the ability of nodes to detect malicious nodes, when a global decision system is applied, is evaluated. As shown in Fig. 2, the rate in existing model [11] varies in each node because of the different local decision, which is based on the road entity. In addition, the rate is very high and reaches 1 in some nodes because the normal node does not meet the malicious node during the simulation time. However, all nodes have the same rate in the proposed model because of global knowledge of malicious nodes even if they do not meet.

In addition, a comparison between the proposed model and existing model [11] is studied. As shown in Fig. 3, low FNR value is achieved by the proposed model where the node can avoid the communication with malicious node even if they meet for the first time. Thus, the improvement rate reaches approximately 74%. As a result of low FNR value, the proposed model achieves the lowest PDR value. Therefore, the improvement in the proposed model is equal

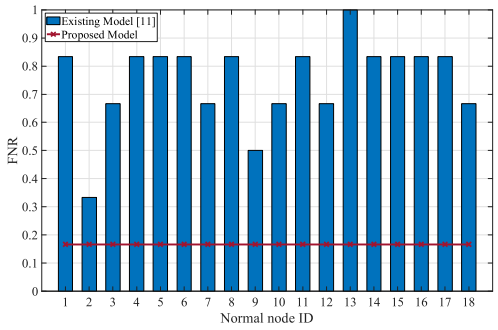


Fig. 2. Rate of non-detected malicious nodes per node in proposed model and existing model [11]

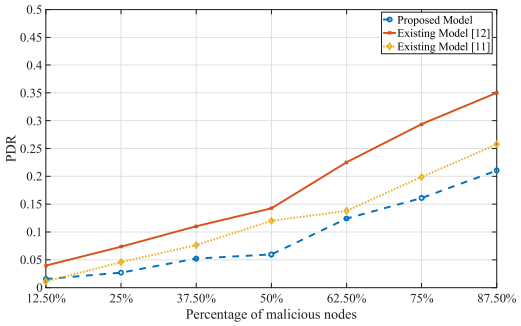


Fig. 4. Effect of various percentage of selective forwarding attackers on PDR

to 52%. As a conclusion, the proposed model could improve the decision accuracy for the nodes that are located in-network coverage.

B. Effect of Selective Forwarding Attack on PDR

In Fig. 4, the PDR with different percentage of malicious nodes is studied. Generally, the PDR is increasing when the percentage of malicious nodes is increasing. In addition, the existing model [12] produces the highest PDR values which results of high FNR. On the other hand, the proposed model has lowest PDR in comparison with [11], [12] which improves the network performance.

VI. Conclusion

In this paper, we proposed a global trust-based model for securing V2X networks against RSU attacks. Various RSU malicious behaviours were considered to study the performance of the proposed model. Multiple experiments were conducted with different percentage of malicious RSUs. Also, we examined how the proposed model improves the accuracy of trust decisions. Comparison results showed that the proposed model provides excellent improvement in FNR values, which is around 74% in comparison with the existing model [11]. In future work, the model will be tested using real-world data, and then we will compare the results with the simulation results.

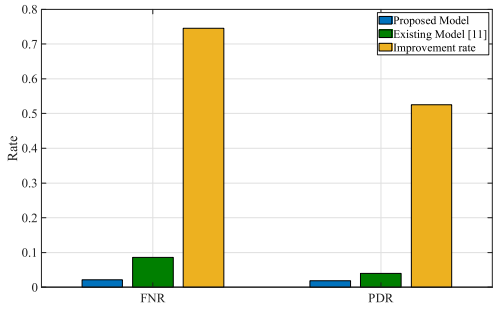


Fig. 3. FNR and PDR in the network for global and distributed decision

References

[1] H. Sedjelmaci and S. M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks," *Computers & Electrical Engineering*, vol. 43, pp. 33–47, 2015.

[2] K. Rostamzadeh, H. Nicanfar, N. Torabi, S. Gopalakrishnan, and V. C. Leung, "A context-aware trust-based information dissemination framework for vehicular networks," *IEEE Internet of Things Journal*, vol. 2, no. 2, pp. 121–132, 2015.

[3] C. A. Kerrache, N. Lagraa, C. T. Calafate, J.-C. Cano, and P. Manzoni, "T-VNets: A novel trust architecture for vehicular networks using the standardized messaging services of ETSI ITS," *Computer Communications*, vol. 93, pp. 68–83, 2016.

[4] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.

[5] C. Sun, J. Liu, X. Xu, and J. Ma, "A privacy-preserving mutual authentication resisting DoS attacks in VANETs," *IEEE Access*, vol. 5, pp. 24 012–24 022, 2017.

[6] L. Zhang, "OTIBAAGKA: A new security tool for cryptographic mix-zone establishment in vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 12, pp. 2998–3010, Dec. 2017.

[7] E. B. Hamida, H. Noura, and W. Znaidi, "Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures," *Electronics*, vol. 4, no. 3, pp. 380–423, 2015.

[8] A. Alnasser, H. Sun, and J. Jiang, "Cyber security challenges and solutions for V2X communications: A survey," *Computer Networks*, vol. 151, pp. 52–67, 2019.

[9] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, 2018.

[10] Y. Hao, Y. Cheng, and K. Ren, "Distributed key management with protection against RSU compromise in group signature based VANETs," in *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*. IEEE, 2008, pp. 1–5.

[11] A. Alnasser, H. Sun, and J. Jiang, "Recommendation-based trust model for vehicle-to-everything (v2x)," vol. 7, pp. 440–450, 2020.

[12] A. M. Shabut, K. P. Dahal, S. K. Bista, and I. U. Awan, "Recommendation based trust model with an effective defence scheme for MANETs," *IEEE Transactions on Mobile Computing*, vol. 14, no. 10, pp. 2101–2115, 2015.

[13] A. Alnasser and H. Sun, "Global roaming trust-based model for V2X communications," in *Accepted for IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2019.