Advances in Intelligent Transportation Systems in Smart Cities - Research Article

International Journal of
Distributed
Sensor Networks

International Journal of Distributed Sensor Networks
2020, Vol. 16(7)
© The Author(s) 2020
DOI: 10.1177/1550147720939372
journals.sagepub.com/home/dsn
SAGE

A hybrid dual-mode trust management scheme for vehicular networks

Ibrahim Abdo Rai, Riaz Ahmed Shaikh and Syed Raheel Hassan

Abstract

Vehicular ad-hoc networks allow vehicles to exchange messages pertaining to safety and road efficiency. Building trust between nodes can, therefore, protect vehicular ad-hoc networks from malicious nodes and eliminate fake messages. Although there are several trust models already exist, many schemes suffer from varied limitations. For example, many schemes rely on information provided by other peers or central authorities, for example, roadside units and reputation management centers to ensure message reliability and build nodes' reputation. Also, none of the proposed schemes operate in different environments, for example, urban and rural. To overcome these limitations, we propose a novel trust management scheme for self-organized vehicular ad-hoc networks. The scheme is based on a crediting technique and does not rely on other peers or central authorities which distinguishes it as an economical solution. Moreover, it is hybrid, in the sense it is data-based and entity-based which makes it capable of revoking malicious nodes and discarding fake messages. Furthermore, it operates in a dual-mode (urban and rural). The simulation has been performed utilizing Veins, an open-source framework along with OMNeT++, a network simulator, and SUMO, a traffic simulator. The scheme has been tested with two trust models (urban and rural). The simulation results prove the performance and security efficacy of the proposed scheme.

Keywords

Vehicular networks, ad-hoc networks, trust management

Date received: 18 February 2020; accepted: 1 June 2020

Handling Editor: Rodolfo Meneguette

Introduction

According to the road safety report released by the World Health Organization (WHO) in 2018, the number of road traffic mortalities was 1.35 million.[1] Implementing vehicular ad-hoc networks (VANETs) may help in reducing some of the road accidents by spreading pertinent information among vehicles.[2] Consequently, drivers can receive warning messages in addition to traffic condition information, which allows them to make the right decision through their driving experience. Furthermore, the advantage of VANETs is that vehicles are equipped with an on-board unit (OBU)[3] operating under IEEE 802.11p which makes it a preferable choice for enhancing intelligent transporting system (ITS).

Information concerning road safety and efficiency is exchanged among vehicles via VANETs. Incorrect information would lead to adverse effects, thereby increasing accidents and traffic congestion. The researchers have addressed the security in VANETs through two different perspectives: cryptography-based and trust-based.[4] The cryptography-based solutions offer a protective shield for VANETs from outsider

Department of Computer Science, King Abdulaziz University, Jeddah, Saudi Arabia

Corresponding author:
Ibrahim Abdo Rai, Department of Computer Science, King Abdulaziz University, Jeddah, 21589 Saudi Arabia.
Email: irai0001@stu.kau.edu.sa

attacks while the trust-based solutions protect VANETs from insider attacks.[5]

Cryptography-based methods maintain messages integrity and afford confidentiality.[6] However, they are incompetent in providing messages quality and reliability[7] or recognizing untrusted nodes.[8] Recently, several VANET models have been developed. However, they experience several limitations and encounter network degradation. Some schemes are unable to ensure message reliability[9,10] or maintain nodes' privacy.[11–14] In addition to that, many solutions rely on central authorities[11–13,15–17] such as roadside units (RSUs) which are costly and susceptible to physical attacks, besides they increase computational complexity.[8]

In this research, we propose a novel trust management scheme for decentralized vehicular networks that overcomes the aforesaid limitations. The scheme is based on a crediting technique and does not rely on other peers or central authorities to ensure message reliability. Moreover, the scheme tackles nodes' legitimacy and message reliability, which qualifies it to be data-oriented and entity-oriented. Furthermore, it operates in a dual-mode: urban and rural environments. The proposed scheme comprises the following characteristics:

- Node crediting: for each sender nodes, the proposed scheme at the receiver node establishes a credit value that is derived from validating the messages received and sender nodes' history. This credit value is prone to increment and decrement based on nodes' behavior.
- Fake source location detection: the scheme is able to verify the source's location based on its coordinates incorporated in the message received. The received messages are accepted if the sender node is located within the accepted range.
- Fake event location detection: the scheme estimates the distance between the sender node and the event based on their location coordinates. Then, it verifies the distance to ensure the correctness of the event location.
- False event time detection: in VANETs, every event has a specific duration and every message has a limited propagation delay. The proposed scheme can assess the received message to ensure that the reported event is within the specified interval and the propagation delay is bounded by the upper and lower pre-defined limit.
- Dual-mode operation: the proposed scheme operates in a dual-mode: urban and rural environments. Two distinct approaches have been developed to tackle the security based on the aspects of each environment, such as the average rate of vehicles per hour and the number of collisions and fatalities.
- Malicious nodes' revocation: every node is given a certain amount of credit. Malicious nodes will incur credit deduction. Once a malicious node's credit reaches zero, it will be revoked.
- Application-wise threshold decision: different threshold limits have been assigned to each application based on application sensitivity from the safety perspective.

The results are relevant to VANET safety and road efficiency applications as vehicles receive a scheme that enables them to have safe driving trips. Consequently, traffic accidents and road congestion will be minimized. The main contributions of our study are as follows:

- An autonomous trust management scheme, for self-organized vehicular networks, is proposed based on a crediting technique. The scheme does not count on network peers or central authorities, for example, RSUs and reputation management centers (RMCs), to ensure message reliability, which makes it a cost-effective solution.
- Two distinct approaches have been developed to operate in different environments: urban and rural. The urban-mode accommodates the traffic safety requirements of urban areas. Similarly, the rural-mode is more adequate for rural territory conditions.

The security analysis besides the simulation results demonstrates the efficiency of our work. The scheme satisfies the security and performance requirements under vehicle-to-vehicle (V2V) communication.

The proposed scheme[i] operates in four phases. In the first phase, the receiver node validates the messages claimed by the sender nodes based on three parameters: sender location, event location, and event time. In the second phase, the scheme measures the reliability of the messages based on two different approaches, urban and rural modes, and simultaneously it updates the history of the sender nodes. The scheme, in the third phase, measures the trust value of each unique message reporting a specific event. Finally, the scheme selects the unique message with the highest trust value and accepts it, if it is above the pre-defined threshold limit.

This article is organized as follows. The related work is explored in section "Related work." In section "Trust management model," the trust management model is discussed in detail. Section "Analysis and evaluation" provides an analysis and evaluation of the proposed solution based on security resiliency and time complexity. In section "Simulation-based analysis and evaluation," simulation-based analysis and evaluation are presented. A qualitative comparison of the proposed method is exhibited in section "Comparison and discussion." Section "Conclusion" concludes the article with our findings and future work.

Related work

Li et al.[15] have proposed a collaborative trust management framework that is based on reputation. During network interaction, nodes share their trust values with a dedicated reputation center, which is used to hold the reputation of all nodes in the network. The reputation center computes nodes' reputation based on their trust statistically and makes it available for any node in the network. If the trust value is not available, the reputation center requests it from a nearby RSU through an encrypted connection. The authors argued that their proposed solution can improve network security. However, the efficiency of the proposed model remains uncertain due to the lack of performance analysis and the relative simulation provided. Moreover, it relies on RSUs, RMCs, and peers feedback to build nodes' reputation.

An intrusion detection model has been developed by Sedjelmaci and Senouci[11] to protect VANETs from attacks. The authors developed a clustering technique that generates clusters in the network. Each cluster is formed of several vehicles and has a cluster head elected based on its trust level. The proposed framework is composed of three intrusion subsystems: local detection that operates at the cluster level, global detection that operates at cluster head level, and global decision that runs at the RSU. This model is centralized and relies on global decision system (GDS) that runs at RSU. In addition, no revocation action is applied to malicious nodes.

Zhang et al.[12] have proposed a trust management scheme that deals with message dissemination and valuation in VANETs. Before any road safety and efficiency message is spread in the network, the scheme assesses the trustworthiness of the message through utilizing the information provided form other peers about it, which allows the scheme to function as a relay of trusted messages. The model is centralized and requires collecting data about nodes from a central authority. Also, the network is prone to network congestion due to the packet relaying mechanism. Moreover, the simulation is limited as it was performed based on a C++ code rather than a professional simulator.

Zhou et al.[13] have developed a security authentication model that incorporates trust evaluation. In order to implement secure authentication, the authors composed the model into two parts: direct and indirect trust assessment. The proposed model is centralized and relies on the authority unit (AU) to determine nodes' trust.

Ltifi et al.[14] have proposed a functional model for managing alerts in the trust management scheme utilizing wireless sensor network (WSN). The authors assumed that every node in the network is equipped with a speed sensor that is connected with WSN. Besides, each vehicle in the network has a distinct role, either as a group leader or a member. The functional model is composed of a trust management scheme and a knowledge base. The authors stated that the model is used for warning and with the presence of any trusted third party. Also, WSN is limited in power, memory, and processing capabilities.

Shaikh and Alzahrani[18] have presented a trust management scheme for ad-hoc networks that focuses on identity anonymous. This method operates in three stages. First, it computes the confidence of messages received from the sender nodes, then calculates the trust value of the messages, and finally accepts the message with the highest trust value. The location verification method in the proposed solution assumed line-of-sight between the sender and the receiver which is not realistic. In addition, it does not incorporate a mechanism to revoke malicious nodes. Therefore, it is prone to an on–off attack.

Kumar and Chilamkurti[16] have presented an intrusion detection model based on learning automata (LA) that were assumed to be installed on vehicles to collect information resulting from vehicles' interconnection over the network. States and transitions in the network are formed using the Markov chain model (MCM). The model is composed of two parts: data collection and intrusion detection. Due to VANETs' ephemeral nature, LA is not an efficient method to detect intrusion in the network. Also, no simulation was performed and no revocation mechanism is applied on malicious nodes.

A trust management scheme has been presented by Chen and Wei[17] to overcome the challenges resulting from the conflict between security and privacy in VANETs. The scheme is based on the integration between the event message in the road and the beacon message of the network so that the message with the higher trustworthiness is selected. The proposed model relies on public key infrastructure (PKI). Also, all messages are encrypted. Therefore, it is susceptible to network performance degradation.

Huang et al.[19] have proposed a trust management model based on nodes' voting. The closer the node to an event the higher the weight it is assigned. There is no method to distinguish between legitimate and malicious nodes. In the case of receiving messages from malicious nodes, relying on those messages is misleading and the result may be catastrophic. Also, it is prone to network attacks as there is no revocation method against malicious nodes.

Gurung et al.[20] have presented a content validation model for VANETs. Each initialized message in the network is assigned a trust value before getting spread over the network. When a message is received from multiple nodes, the model computes its trustfulness based on content similarity, content conflict, and route similarity. No simulation was provided. Also, the authors stated that the model lacks in-depth message analysis and needs accuracy improvement.

Cui et al.[8] have proposed a reputation system in addition to a message authentication framework and protocol for 5G-VANET (reputation system–based lightweight message authentication framework (RSMA)). The reputation system is managed by a trusted authority (TA) and operates in three phases. In the first phase, the TA collects and filters the valid feedbacks, and then classifies them in accordance with the type of the message (true or fake). In the second phase, the reputation score for the target vehicle is calculated; the greater feedback the higher reputation score is achieved. Finally, the reputation score is updated and sent to the global reputation center. However, this work is based on TA and is fundamentally different from self-organized VANETs we focus on.

To secure the communication between vehicles in VANETs, Zhang et al.[21] have proposed a scheme based on the Chinese remainder theorem that offers secure authentication and maintains nodes' privacy. The network model is composed of TAs, RSUs, and vehicles equipped with OBUs. However, the proposed scheme is totally centralized and relies on central authorities such as RSUs and TAs.

Trust management model

In this section, we introduce the proposed trust management model as shown in Figure 1. The model is based on V2V communication and does not rely on central authorities, for example, RSUs or RMCs. A typical V2V communication model is illustrated in Figure 2, wherein vehicles exchange messages with others in the close vicinity. Each vehicle is equipped with an OBU to facilitate the communication process.

Our method operates in four phases. In the first phase, the receiver node validates the message claimed by the sender node. In the second phase, the message reliability is measured based on two different approaches, urban and rural modes, and simultaneously it updates the history of the sender node. The scheme, in the third phase, measures the trust value of the unique message reporting a specific event. Finally, the scheme selects the unique message with the highest trust value and accepts it, if it is above the pre-defined threshold limit. The following sections discuss the aforementioned phases.

Claim validation

The model enables the receiver nodes to validate the message claimed by the sender nodes utilizing three factors: the source's location (L_s), the event location (L_e), and the event time (T_e).

Source's location. We assume the propagated message carries the coordinates of the sender node. The distance between the sender and the receiver nodes is estimated using standard equation (1)

$$d_s = \sqrt{(x_s - x_r)^2 + (y_s - y_r)^2} \tag{1}$$

where d_s is the distance between the sender and the receiver nodes, x_s and y_s represent the claimed sender's location coordinates, and x_r and y_r represent the receiver's location coordinates.

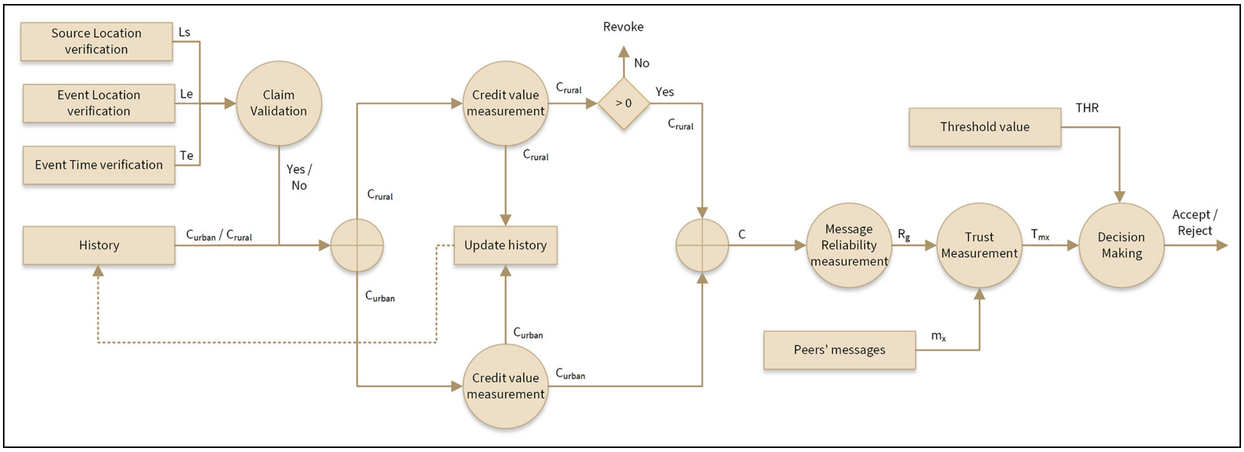


Figure 1. The proposed scheme.

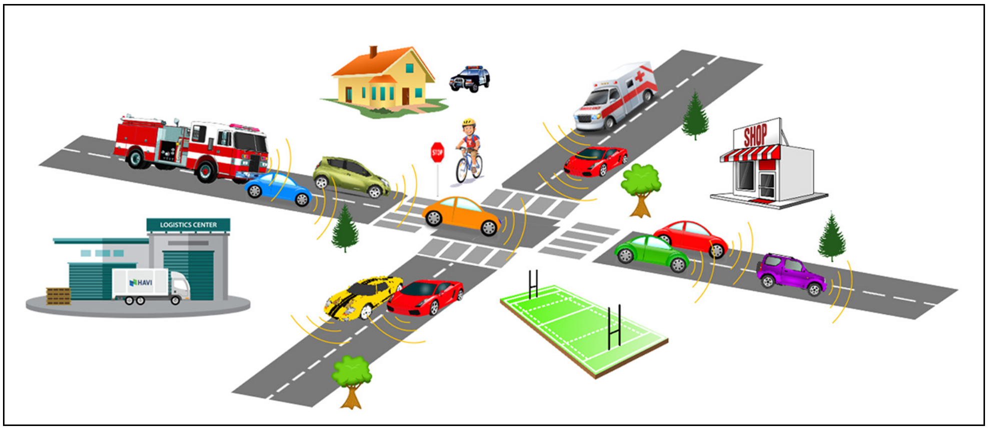


Figure 2. A typical V2V communication model.

Algorithm 1. Claim validation.

```
int function $V_c(x_s, y_s, x_r, y_r, x_e, y_e, t_s, t_r)$
Let $d_m$ is the maximum distance a node can communicate
$d_s = \sqrt{(x_s - x_r)^2 + (y_s - y_r)^2}$
if $(!(0 < d_s \leqslant d_m + \varphi))$
    return 0
end if
$d_e = \sqrt{(x_s - x_e)^2 + (y_s - y_e)^2}$
if $(!(0 < d_e \leqslant d_m + \varphi))$
    return 0
end if
if $(!(min \leqslant (t_r - t_e) \leqslant max))$
    return 0
end if
return 1
end function
```

The maximum distance a vehicle can communicate d_m is 1000 m.[22] Therefore, we can verify the source's location using equation (2). An error margin φ is obtained for a tolerable result

$$L_s = \begin{cases} 1 & 0 < d_s \leqslant d_m + \varphi \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

The model only processes the messages received from sender nodes on the same road. This can be enforced by validating the road identifier of the sender and the receiver vehicles.

Event location. When an event occurs in the network, such as road accidents or traffic congestion, vehicles disseminate these events to other nodes including the event location.[23] The distance between the sender node and the event d_e is estimated through equation (3)

$$d_e = \sqrt{(x_s - x_e)^2 + (y_s - y_e)^2} \tag{3}$$

where x_s and y_s represent the coordinates of the sender's location while x_e and y_e represent the coordinates of the event location.

Equation (4) is developed to verify the location of the event. An error margin φ is obtained for a tolerable result when comparing d_e with the maximum distance d_m a vehicle can reach

$$L_e = \begin{cases} 1 & 0 < d_e \leqslant d_m + \varphi \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

Event time. A message is generated when requested by an application at the sender node then disseminated to the nearby vehicles.[24] According to Soleymani et al.,[25] the arrival time of a notification message can be calculated using equation (5)

$$t_r = t_e + \frac{d}{c} \tag{5}$$

where t_r represents the time the receiver node receives the message, t_e is the time at the sender node when the event is generated assuming that the event time and the sending time are the same, and d is the distance between the sender and the receiver nodes.

According to Wang et al.,[26] the upper and lower limit of the propagation delay of IEEE 802.11p can range from 253.5 μs to 1 s at 6 Mbps for a payload size of 500 bytes. Therefore, we could estimate the propagation delay in equation (6); the result is true if the sender node provides the correct event time

$$T_e = \begin{cases} 1 & min \leqslant (t_r - t_e) \leqslant max \\ 0 & \text{otherwise} \end{cases} \tag{6}$$

Overall, we have three parameters: the sender location L_s, the event location L_e, and the event time T_e; consequently, we could validate the claimed message provided by the sender nodes as shown in Algorithm 1.

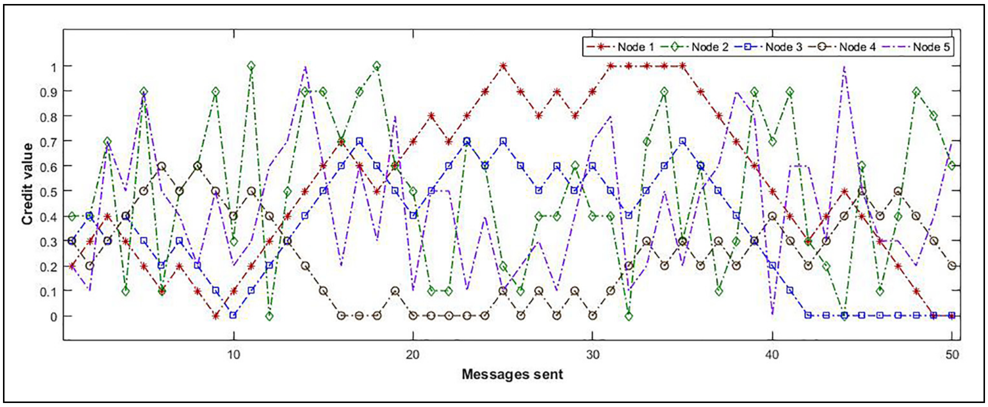


Figure 3. The implementation of equation (7) in MATLAB with five nodes.

Message reliability

The proposed model can operate in two different environments: urban and rural as per the selected mode. In the previous section, we have discussed how the messages are endorsed based on three parameters: the source's location, event location, and event time. In this section, we focus on two approaches implemented in the proposed scheme to calculate the reliability of the messages.

A study of the traffic flow by Sampson[27] shows that the average rate of the vehicles in urban areas is 12,629 vehicles per hour while in rural areas, the rate is 9418. However, traffic collisions are more in urban roads while fatalities are more in rural territories according to the Centers for Disease Control and Prevention (CDC) in Atlanta.[28] Therefore, the first approach is developed to meet the requirements of urban areas. Similarly, the second approach is more adequate for rural areas.

Urban mode. When a vehicle receives a message from a sender node, the message is evaluated, as in the first phase, then, a credit value is assigned to the sender based on the evaluation result. In urban areas, the rate of the vehicles and the traffic collisions are massive. Therefore, the credit value should be elastic enough to accommodate these properties.

The receiver node, on its OBU, maintains the credit values of the sender nodes during network interaction. The credit value ranges from (0.0) to (1.0) and is prone to increment and decrement based on the node's behavior.

Equation (7) is used to calculate the credit value. The new credit value of a node C_{urban} is influenced by the current value $C_{urban_{i-1}}$ and the claim validation V_c result. The progression factor δ controls the rise and the drop amount of the current credit value. Equations (8) ensures that the final credit value C is retained in the pre-defined interval

$$C_{urban} = C_{urban_{i-1}} + (V_c \times 2\delta) - \delta \tag{7}$$

$$C = \begin{cases} 0 & C_{urban} < 0 \\ C_{urban} & 0 \leqslant C_{urban} \leqslant 1 \\ 1 & C_{urban} > 1 \end{cases} \tag{8}$$

The graph in Figure 3 illustrates the implementation of equation (7) in MATLAB wherein the credit values of five sender nodes increase and decrease based on nodes' behavior.

Rural mode. In rural regions, traffic hazards are severe.[29–33] Therefore, the second approach is more convenient to minimize the risk very effectively. The receiver node assigns an initial credit value β to each sender node. The value of β is defined by the trust model and may range from (0.1) to (1.0). When a sender node sends a false message, its claim validation (V_c) yields zero, consequently, its credit value C_{rural} is decremented by α as shown in equation (9). Whenever the credit value is updated, it is validated by equation (10) to obtain the final credit C of the node. If the value of C_{rural} reaches zero, the node is revoked

$$C_{rural} = \begin{cases} C_{rural_{i-1}} - \alpha & V_c = 0 \\ C_{rural_{i-1}} & \text{otherwise} \end{cases} \tag{9}$$

$$C = \begin{cases} C_{rural} & 0 < C_{rural} \leqslant \beta \\ \text{revoke} & C_{rural} = 0 \end{cases} \tag{10}$$

Once the claim validation is performed and the sender node's credit value is decided, the message reliability R_g is calculated using equation (11) based on the selected mode

$$R_g = C \times V_c \tag{11}$$

The result of (R_g) will be used in calculating the message trust as described in the next section.

Message trust

The receiver node receives messages from multiple sender nodes for a specific event. Suppose we have an event E and we received several messages from n nodes related to this event. The set of all unique messages M related to the event E is

$$M = \{m_1, m_2, \ldots, m_r\} \tag{12}$$

To calculate the trust value of each unique message, we developed equation (13)

$$T_{m_x} = \frac{\sum_{i=1}^{n_{m_x}} R_{g_i}}{\sum_{i=1}^{n} R_{g_i}} \tag{13}$$

where T_{m_x} represents the trust value of each unique message in M, n_{m_x} is the number of nodes that send the same message m_x, $\sum_{i=1}^{n_{m_x}} R_{g_i}$ is the total message reliability values for all nodes that send the message m_x, and $\sum_{i=1}^{n} R_{g_i}$ represents the total message reliability values for all nodes that contribute to the event E.

Decision-making

After calculating the trust value of each unique message, the model selects the message m_x with the highest trust value utilizing equation (14). The trust value of the selected message is evaluated through equation (15); thereby, it is accepted if it has a trust value greater than the pre-defined threshold, otherwise, it will be rejected. In case, multiple messages have the same trust value, they will be discarded too

$$T_{m_x} = \max\{T_{m_1}, T_{m_2}, \ldots, T_{m_r}\} \tag{14}$$

$$D_{m_x} = \begin{cases} \text{accept} & T_{m_x} > THR \\ \text{reject} & \text{otherwise} \end{cases} \tag{15}$$

The threshold value for trusting a message depends on the application types. There are three types of applications in VANETs: safety applications, traffic efficiency applications, and infotainment applications.[34] According to the importance of the messages disseminated by the application, they are classified into three categories: very sensitive, sensitive, and normal. Each category is given a threshold level. Application types along with their categories and threshold levels are shown in Table 1.

Table 1. Application types of pre-defined thresholds.

Application type	Category	Threshold level
Safety	Very sensitive	0.60
Traffic efficiency	Sensitive	0.55
Infotainment	Normal	0.5

Analysis and evaluation

In this section, we evaluate the proposed scheme with respect to security resiliency and privacy, in addition to the performance.

Security resiliency analysis

The proposed scheme focuses on the trustworthiness messages, in addition to the credit values of the nodes. Some important definitions of the proposed model are as follows:

Definition 1. A message is considered invalid if it matches any of the following conditions:

- False source's location is detected.
- False event location is detected.
- Fake event time is detected.

Definition 2. A malicious node is a node that disseminates bogus messages.

The distinct features of the proposed model are as follows:

- Assuring the correctness of the messages received from the sender nodes.
- Reducing or eliminating the influence of the malicious nodes by assigning them a lower credit value.
- Assigning higher reliability value to truthful messages.
- Selecting messages with the highest trust values.
- Maintaining the privacy of the interacted nodes.

The first feature that the proposed model provides is assuring the correctness of the messages received from the sender nodes through validating the received messages based on three factors: sender location (L_s), event location (L_e), and event time (T_e). If the value of any of the aforementioned factors is incorrect, the validation function yields zero; hence, the received messages are invalid.

Claim 1. The proposed scheme can detect fake source's location.

Proof. According to equation (2), the distance between the sender and the receiver nodes is validated as follows

$$L_s = \begin{cases} 1 & 0 < d_s \leq d_m + \varphi \\ 0 & \text{otherwise} \end{cases}$$

The location provided by the sender node is accepted if the sender node has provided the correct coordinates. Suppose the sender node claims to be $d_m + x$ away from the receiver node, and $x>0$, in this case $d_s = d_m + x + \varphi$. The maximum distance between two nodes in the network is d_m. Therefore, the result will be

$$0 < d_m + x + \varphi \leq d_m + \varphi$$

The result contradicts with equation (2); therefore, the location of the sender node is considered invalid.

Claim 2. The proposed model can detect false event location.

Proof. When an event is reported during network interaction, the receiver node receives a message incorporating the event location. The location of the event can be evaluated utilizing equation (4)

$$L_e = \begin{cases} 1 & 0 < d_e \leq d_m + \varphi \\ 0 & \text{otherwise} \end{cases}$$

Assume the sender node claims the event is located $d_m + r$ away from its location and $r>0$. Hence, $d_e = d_m + r$. Since the maximum distance a node can reach is d_m, the result will be

$$0 < d_m + r + \varphi \leq d_m + \varphi$$

Since $d_m + r > d_m$, the location of the event is incorrect. Therefore, the message is invalid and it is rejected.

Claim 3. The proposed trust model is able to detect false event time.

Proof. From equation (5), when a message is received at a time t_r, we know that the event time t_e and the sending time are approximately the same

$$t_r = t_e + \frac{d}{c}$$

The propagation time of the message is determined by equation (6)

$$T_e = \begin{cases} 1 & min \leq (t_r - t_e) \leq max \\ 0 & \text{otherwise} \end{cases}$$

Suppose a node reported a false event time, in this situation we have two cases

$$1.(t_r - t_e) < minor$$
$$2.(t_r - t_e) > max$$

Any of the two cases contradicts with equation (6); therefore, the verification yields zero and the event time is considered invalid.

Claim 4. The proposed scheme assigns lower credit values to malicious nodes.

Proof. Suppose we have two nodes, a legitimate and a malicious, and the credit values of the legitimate node C_{urban_t} and the malicious node C_{urban_m} are initially equal

$$C_{urban_t} = C_{urban_m} = x \quad x \in \mathbb{Q}|0 \leq x \leq 1$$

Over time, both nodes interact with others in the close vicinity. The credit values of the legitimate node C_{urban_t} and the malicious node C_{urban_m} assigned by the model after network interaction should be as follows

$$C_{urban_t} > C_{urban_m}$$

Equation (7) calculates the credit value of the sender nodes. The claim validation V_c of the legitimate node is always true while it is always false for the malicious node

$$C_{urban} = C_{urban_{i-1}} + (V_c \times 2\delta) - \delta$$

Let $\delta = 0.1$ accordingly

$$C_{urban_t} = x + (1 \times 0.2) - 0.1 = x + 0.1$$
$$C_{urban_m} = x + (0 \times 0.2) - 0.1 = x - 0.1$$

Consequently

$$x + 0.1 > x - 0.1$$

Therefore, malicious nodes will always have lower credit values.

Claim 5. True messages have a higher reliability value.

Proof. From equation (11), the message reliability R_g is computed as follows

$$R_g = C \times V_c$$

Suppose the receiver node receives two messages, a true message m_t and a fake message m_f, from legitimate and malicious nodes, respectively. Assuming both having the same credit value $C_t = C_f$. Since the claim validation is always 1 for the true message and is always 0 for the fake message, the true message will have a higher reliability value. We can represent this as

$$C_t \times V_c > C_f \times V_c \Rightarrow$$
$$C_t \times 1 > C_f \times 0 \Rightarrow C_t > 0$$

Therefore, the reliability of the true message is greater than that of the fake message

$$R_{g_t}>R_{g_f}$$

Claim 6. Only messages with the highest trust values are selected.

Proof. Suppose there is an event E, and the receiver node receives two types of messages m_1 and m_2 sent by legitimate and malicious nodes, respectively

$$T_{m_x}=\frac{\sum_{i=1}^{n_{m_x}} R_{g_i}}{\sum_{i=1}^{n} R_{g_i}}$$

Equation (13) is used to find the trust value of each message. Since m_1 has a greater trust value than m_2

$$T_{m1}>T_{m2}$$

We can write this as

$$\frac{\sum_{i=1}^{n_{m_1}} R_{g_i}}{\sum_{i=1}^{n} R_{g_i}}>\frac{\sum_{i=1}^{n_{m_2}} R_{g_i}}{\sum_{i=1}^{n} R_{g_i}}$$

Multiplying both sides by

$$\sum_{i=1}^{n} R_{g_i}$$

We get

$$\sum_{i=1}^{n_{m_1}} R_{g_i}>\sum_{i=1}^{n_{m_2}} R_{g_i}$$

In claim 5, we have proven that the reliability of the message sent by a malicious node m_2 is always zero. Therefore, the following result is always true

$$\sum_{i=1}^{n_{m_1}} R_{g_i}>0$$

Consequently, m_1 is selected as in equation (14)

$$T_{m_x}=\max\{T_{m_1},T_{m_2},\ldots,T_{m_r}\}$$

Claim 7. Messages having the same trust value will be discarded.

Proof. Suppose there are multiple unique messages of an event E. According to equation (12), we can write this as follows

$$M=\{m_1,m_2,\ldots,m_r\}$$

In this scenario, we use equation (13) to calculate the trust value of each unique message

$$T_{m_x}=\frac{\sum_{i=1}^{n_{m_x}} R_{g_i}}{\sum_{i=1}^{n} R_{g_i}}$$

From the definition of equation (13), T_{m_x} represents the trust value on the message m_x, and $\sum_{i=1}^{n_{m_x}} R_{g_i}$ and $\sum_{i=1}^{n} R_{g_i}$ represent the total message reliability for all nodes that send the message m_x and the total message reliability for all nodes that contribute to the event E, respectively. So, the trust value of any particular event can be calculated as

$$T_m=T_{m_1}+T_{m_2}+\cdots+T_{m_{\mathrm{r}}}=1 \tag{16}$$

where $T_{m_1}, T_{m_2},$ and T_{m_r} represent the trust values on messages $m_1, m_2,$ and m_r, respectively. In case there are two messages $m_1$and m_2 having the same trust value, this gives the following result

$$T_{m_1}=T_{m_2}=0.5$$

The value 0.5 is not greater than the minimum acceptable pre-defined threshold (0.5). Therefore, both messages will be discarded according to equation (15). This feature is also applicable when we have more than two messages ($r>2$)

$$D_{m_x}=\begin{cases}\text{accept} & T_{m_x}>THR\\ \text{reject} & \text{otherwise}\end{cases}$$

Claim 8. The proposed model maintains the nodes' privacy.

Proof. The proposed model is based on V2V communication wherein messages are exchanged among nodes without being exposed to third parties such as RSUs or advertising roadside services. Moreover, the credit values of the sender nodes are maintained at the OBU. Therefore, the proposed model preserves the privacy of the nodes during network interaction.

Table 2 represents the multiple scenarios that may take place when messages are disseminated in the V2V network. In the first scenario, the sender node provides a valid message; thereby, its trust value is within the acceptable range. In other scenarios, the sender nodes offer rigged messages. The model detects the bogus messages once a constraint is met. In the third scenario,

Table 2. Security analysis of the proposed scheme.

Scenario	Node's provided			Model validation			Trust value	Unfulfilled constraints
	d_s	d_e	t_e	L_s	L_e	T_e		
1	T	T	T	1	1	1	$0<T_{m_x} \leqslant 1$	Fair
2	T	T	F	1	1	0	0	$(t_r - t_e)\langle min, or(t_r - t_e)\rangle max$
3	T	F	T	1	1	1	$0<T_{m_x} \leqslant 1$	Deception
4	T	F	F	1	1	0	0	$(t_r - t_e)\langle min, or(t_r - t_e)\rangle max$
5	F	T	T	1	1	0	0	$d_s>d_m + \varphi$
6	F	T	F	1	1	0	0	$d_s>d_m + \varphi\&(t_r - t_e)\langle min, or(t_r - t_e)\rangle max$
7	F	F	T	1	1	0	0	$d_s>d_m + \varphi$
8	F	F	F	1	1	0	0	$d_s>d_m + \varphi\&(t_r - t_e)\langle min, or(t_r - t_e)\rangle max$

the sender node deceives the model by providing a false event location. This is true because the model restricts both the sender node and the event location to be within the allowable range. However, the model tackles this issue when unique messages are compared.

Time complexity analysis

In the proposed model, there are four main operations: claim validation, message reliability measurement, trust measurement, and decision-making. In this section, we analyze the time complexity of every main operation. Then, we derive the time complexity of the whole model.

In the claim validation, the model verifies the source's location through equations (1) and (2). There are seven and four execution steps in equations (1) and (2), respectively. In event location verification, equation (3) has seven execution steps and equation (4) has four execution steps. Equation (6) in event time verification has four execution steps. Subsequently, there are 26 execution steps in the claim validation.

In message reliability measurement, there are five execution steps in equation (7), five execution steps in equation (8), and two execution steps in equation (11). In total, there are 12 execution steps in measuring the reliability of the messages.

As a result, 38 execution steps are performed on every received message in the first two operations. In the case of receiving n messages for a particular event, there will be $38n$ execution steps. Therefore, the time complexity is $O(n)$.

The trust measurement operation is performed on every unique message for a particular event. In equation (12), M represents the set of all unique messages in an event E when the receiver node receives multiple messages from n nodes with the cardinality of $|M| = r$

$$M = \{m_1, m_2, \dots, m_r\}$$

To calculate the trust of a unique message m_x received from n_{m_x} nodes using equation (13), the model requires $n_{m_x} + n + 2$ execution steps

$$T_{m_x} = \frac{\sum_{i=1}^{n_{m_x}} R_{g_i}}{\sum_{i=1}^{n} R_{g_i}}$$

In the worst case, all messages in M will be unique, thereby $r = n$. Consequently, the number of execution steps required for the entire event is

$$(n_{m_x} + n + 2)_1 + (n_{m_x} + n + 2)_2 + \cdots \\ + (n_{m_x} + n + 2)_{r-1} + (n_{m_x} + n + 2)_r = 3n$$

Therefore, the time complexity of trust measurement is $O(n)$.

The last main operation in the proposed solution is decision-making. In this operation, the model utilizes equation (14) to obtain a unique message with the maximum trust value. Then, it decides to accept or reject the message based on the pre-defined threshold. Several searching algorithms can be used, such as linear search and binary search. The last algorithm requires sorted elements.[35] So, the time complexity of decision-making is $O(n)$.

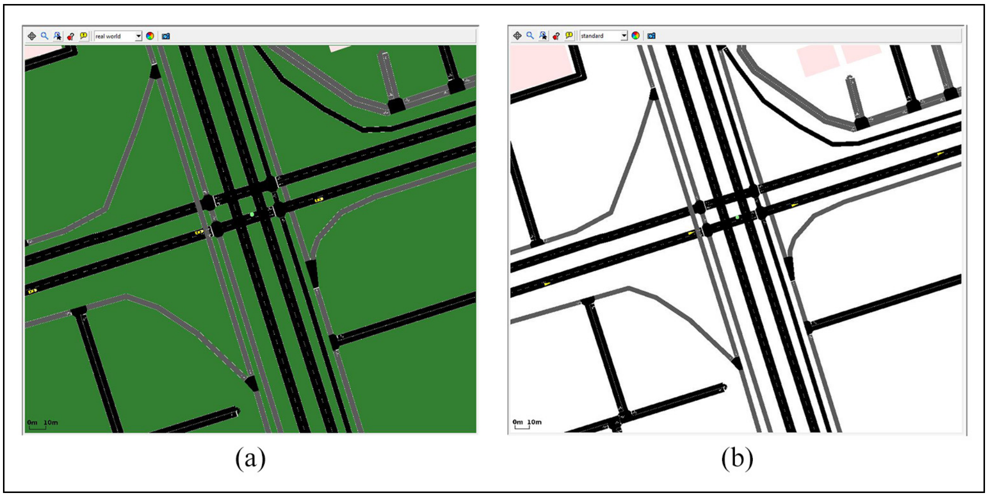
Accordingly, all four main operations: claim validation, message reliability measurement, trust measurement, and decision-making have a time complexity of $O(n)$. Therefore, the proposed scheme is linear.

Simulation-based analysis and evaluation

In this section, we study the performance of the proposed trust model based on four metrics: travel time, CO_2 emissions, communication overhead, and accuracy.

The simulation is conducted utilizing veins[36] as a V2V open-source framework along with OMNeT++,[37] as a network simulator, and SUMO,[38] as a traffic simulator. The map of Jeddah, Saudi Arabia is imported from OpenStreetMap[39] and converted into SUMO network using python scripts.

In the road map, 100 vehicles were deployed with 50% legitimate nodes. Three distinct VANET



(a) (b)

Figure 4. Depicts two different views of a simulation snapshot: (a) a SUMO real world view map and (b) a SUMO standard view map.

applications are created to facilitate the communication between vehicles: a plain application (PA), an urban-trust-model (UTM) application, and a rural-trust-model (RTM) application.

In the first application, the communication between vehicles takes place without any trust model being implemented. In the second application, the UTM is placed between the application layer and the network transport layer. In the wireless access in vehicular environment (WAVE) standards, the IEEE 1609.3 serves the network and the transport layers.[40,41] In the third application, the RTM with the malicious-node-revocation functionality is implemented between the two aforementioned layers.

Each application is capable of exchanging three types of messages: safety, traffic efficiency, and infotainment messages. An adversary model is developed where malicious vehicles attack the network by disseminating bogus messages, thereby affecting vehicles in the close vicinity.

In each application, five scenarios are performed. The percentage of malicious vehicles is 10% and 20% in the first and the second scenarios, and so forth until it reaches 50% in the fifth scenario. Table 3 shows the details of the simulation parameters.

Three applications are simulated, and the results of the four metrics (the travel time, the CO_2 emissions, the communication overhead, and the accuracy) are recorded. Figure 4 shows the snapshots of the simulation run of the Jeddah map.

Table 3. Simulation parameters.

Simulation details	
Simulation time	1000 s
Number of vehicles	100
Simulation area	5.62 km × 3.22 km
Framework and simulators	
Network simulator	OMNeT + + 5.3
Traffic simulator	SUMO 0.30.0
V2V framework	Veins 4.7
MAC environment	
MAC protocol	IEEE 1609.4
Network and transport layer	IEEE 1609.3
Radio propagation model	Free space loss
Radio frequency	5.8 GHz
Transmission power	13 dBm
Receive sensitivity	−82 dBm
Maximum transmitted distance	1000 m
Trust model (urban)	
Initial credit value	0.0
Maximum credit value	1.0
Minimum credit value	0.0
Progression factor	±0.1
Trust model (rural)	
Initial credit value	0.3
Maximum credit value	0.3
Minimum credit value	0.1
Progression factor	±0.1

V2V: vehicle-to-vehicle; MAC: medium access control; IEEE: Institute of Electrical and Electronics Engineers.

Figure 5 illustrates the travel time of the three applications. It can be seen that vehicles have less travel time over the RTM. We observed that when we have 50% malicious nodes, the PA attains 20% and 23% higher travel time as compared to the UTM and the RTM. The number of malicious nodes is increased by 10% each time. However, the travel time is always kept to the minimum.

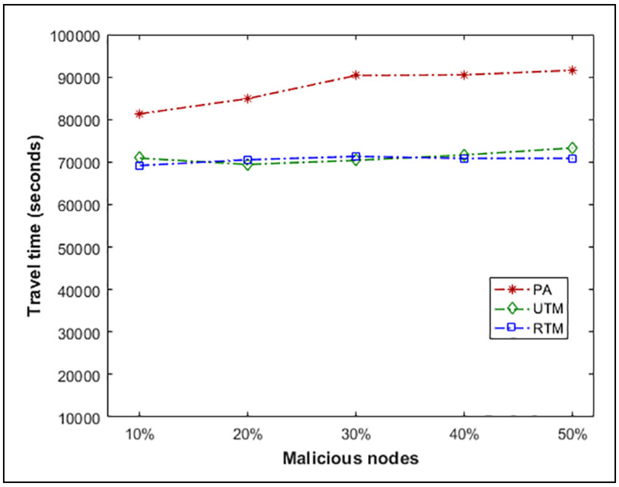


Figure 5. Travel time in seconds.

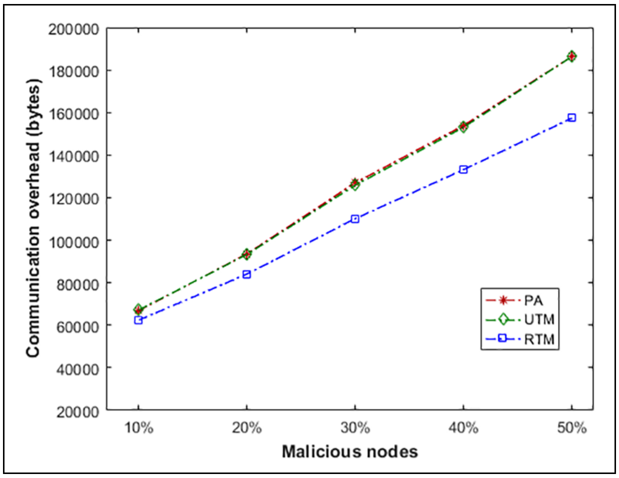


Figure 7. Communication overhead in bytes.

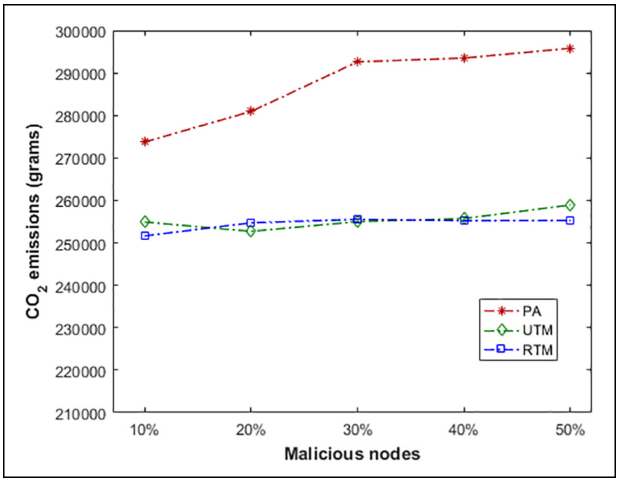


Figure 6. CO_2 emissions in grams.

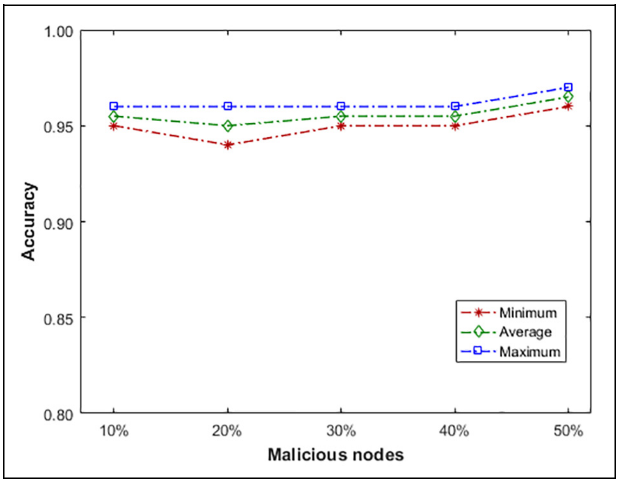


Figure 8. Accuracy of the proposed solution.

The CO_2 emissions are depicted in Figure 6. We perceived that the UTM and the RTM perform 12% and 14% better than the PA. Minimizing CO_2 emissions has a positive impact on reducing global atmospheric temperatures and ocean acidification, in addition to decreasing the factors threatening human health.[42,43]

Figure 7 highlights the communication overhead, it can be observed that the RTM performs 16% better than the UTM and the PA. This is because the RTM is able to revoke non-legitimate nodes. More malicious nodes are injected in each run. However, the RTM is able to abolish them and only allows the trusted nodes. As a result, the communication overhead is reduced.

Figure 8 shows the overall accuracy of the proposed scheme. The accuracy is calculated using equation (17)[44]

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{17}$$

The proposed scheme acquires a minimum accuracy of 94% when the ration of malicious vehicles is 20%. Moreover, it obtains 97% as the highest value of accuracy when the percentage of malicious nodes reaches 50%.

Comparison and discussion

In this section, the proposed trust management scheme is compared with 10 different schemes to perform a qualitative comparison. The followings are the selected parameters along with their definition:

- Fake source location detection: a node shares its location when it interacts with the other adjacent nodes. The trust model should be capable to estimate and verify the sender node's location, thereby accepting the correct information, and thus relying only on the valid received messages.

- Fake event location detection: when an event occurs, it is reported by the nodes in the network. Malicious nodes may disseminate fake event location to benefit from it. The trust model should be able to estimate and verify the location of the event provided by the sender node.
- Fake event time detection: events in VANETs trigger vehicles to send notifications, thereby warning close by vehicles. A message is generated and sent when requested by an application at the sender node.[24] The trust model should be capable to estimate and verify the time of the event to accept the true time and discard the false one(s).
- Node crediting: malicious nodes that disseminate fake messages will not desist as long as they can benefit from so doing. Applying a credibility metric, however, could eliminate their influence on the network.
- Malicious nodes' revocation: the trust model should be able to maintain the interaction history of the nodes and to revoke some when they meet a certain constraint.
- Data-based: known as event-based, and puts emphasis on assessing the data received during network interaction.[45] The trust management solutions should focus on the data as they provide real-time information that is very essential to make a decision.
- Entity-based: focuses on interacted nodes by evaluating their activities.[45] A good trust management model builds messages trust with consideration to the sender nodes and their behavior. A sender node could be judged by its behavior during network interaction.
- Privacy: defined as: "The state of being free from public attention."[46] The trust model should provide privacy by not exposing private information to other peers during network interaction while messages are exchanged between nodes.
- Dynamics: the rate of nodes that join and leave the network is high which makes VANETs a very dynamic network. The average speed of a highway is 100 km/h.[47] The trust model should be dynamic to cope with the dynamic nature of VANETs.
- Scalability: a system is scalable if it is capable to incorporate new nodes without losing data and encountering performance degradation.[48–50] The trust management models should be scalable to receive the essential data used in building nodes' trust.
- Decentralization: decentralized trust management schemes are distributed schemes that do not rely on a central authority. Such schemes have a high chance to succeed.[50] Therefore, trust management schemes should be distributed and less dependent on central authorities.

Table 4. Security analysis of the proposed model.

Parameters	Li et al.[15]	Sedjelmaci and Senouci[11]	Zhang et al.[12]	Zhou et al.[13]	Ltifi et al.[14]	Shaikh and Alzahrani[18]	Kumar and Chilamkurti[16]	Chen and Wei[17]	Huang et al.[19]	Gurung et al.[20]	Proposed scheme
Node crediting											√
Dual-mode operation											√
Malicious node revocation											√
Application-wise threshold decision											√
Hybrid (data- and entity-based)											√
Fake source location detection						√					√
Fake event location detection						√					√
Fake event time detection						√					√
Privacy						√		√		√	√
Dynamics	√	√	√	√	√	√	√	√	√	√	√
Scalability	√	√	√	√	√	√	√	√	√	√	√
Decentralization					√	√			√	√	√

Table 4 illustrates the qualitative comparison between the proposed scheme and 10 other schemes. The proposed scheme is the only scheme that is capable of:

- Maintaining nodes' credit.
- Operating in a dual-mode.
- Revoking malicious nodes.
- Maintaining a dynamic threshold selection.
- Operating as a hybrid model.

From Table 4, only Shaikh and Alzahrani,[18] Chen and Wei,[17] Gurung et al.,[20] and our proposed model can protect nodes' privacy. Scalability and dynamics are presented in all proposed models. Decentralization is attained by Ltifi et al.,[14] Shaikh and Alzahrani,[18] Huang et al.,[19] Gurung et al.,[20] and our model. Node crediting, dual-mode operation, malicious nodes' revocation, dynamic threshold selection, and operating as a hybrid model are only obtained in our proposed scheme.

Conclusion

Assuring message reliability and nodes' credibility without relying on other peers or expensive central authorities, such as RSUs, are some of the most challenging issues in VANETs. Existing trust management solutions do not tackle these challenges in the best manner. Furthermore, none of the proposed schemes operate in both urban and rural environments. In this research, we have developed a novel cost-effective trust management scheme that overcomes the aforementioned limitations. The scheme does not rely on other peers or central authorities to ensure message reliability and nodes' credibility, thereby allowing drivers to make safe decisions based on message quality. Moreover, it is hybrid and is able to revoke malicious nodes. Simulation results show significant improvement in reducing travel time, CO_2 emission, and communication overhead. In addition, the proposed scheme merits an accuracy level in the range of 94% and 97%. The future work is to embed the proposed scheme to real vehicles to compare the experimental and simulation results.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Note

i. This study is an extended version of our paper entitled "A Credit-Based Trust Model for VANETs" which has been accepted for the publication in the Future Technologies, Conference, Springer, Vancouver, 2020.

ORCID iDs

Ibrahim Abdo Rai https://orcid.org/0000-0002-4029-2322
Riaz Ahmed Shaikh https://orcid.org/0000-0001-6666-0253
Syed Raheel Hassan https://orcid.org/0000-0003-4027-3903

References

1. World Health Organization. *Global status report on road safety 2018: summary*. Geneva: World Health Organization, 2018.
2. Thayananthan V and Shaikh RA. Contextual risk-based decision modeling for vehicular networks. *Int J Comput Netw Inf Secur* 2016; 8: 1–9.
3. Dhamgaye A and Chavhan N. Survey on security challenges in VANET. *Int J Comput Sci Netw* 2013; 2: 88–96
4. Kerrache CA, Lakas A and Lagraa N. Detection of intelligent malicious and selfish nodes in VANET using threshold adaptive control. In: *2016 5th international conference on electronic devices, systems and applications (ICEDSA)*, Ras Al Khaimah, United Arab Emirates, 6–8 December 2016, pp.1–4. New York: IEEE.
5. Kerrache CA, Calafate CT, Cano J-C, et al. Trust management for vehicular networks: an adversary-oriented overview. *IEEE Access* 2016; 4: 9293–9307.
6. Saini R and Khari M. Defining malicious behavior of a node and its defensive techniques in ad hoc networks. *Int J Smart Sens Ad Hoc Netw* 2011; 1: 17–20.
7. Shaikh RA, Jameel H, D'Auriol BJ, et al. Group-based trust management scheme for clustered wireless sensor networks. *IEEE Trans Parallel Distrib Syst* 2008; 20: 1698–1712.
8. Cui J, Zhang X, Zhong H, et al. RSMA: reputation system-based lightweight message authentication framework and protocol for 5g-enabled vehicular networks. *IEEE Internet Thing J* 2019; 6: 6417–6428.
9. Ullah K, Jaimes L, Yokoyama RS, et al. Advertising roadside services using vehicular ad hoc network (VANET) opportunistic capabilities. In: *2015 4th international conference on advances in vehicular systems, technologies and applications (VEHICULAR 2015)*, St. Julians, 11–16 October 2015, pp.7–13. Wilmington: IARIA.
10. Mavromatis I, Tassi A, Piechocki RJ, et al. Efficient V2V communication scheme for 5G MmWave hyper-connected CAVs. In: *2018 IEEE international conference on communications workshops (ICC workshops)*, Kansas City, MO, 20–24 May 2018, pp.1–6. New York: IEEE.
11. Sedjelmaci H and Senouci SM. An accurate and efficient collaborative intrusion detection framework to secure vehicular networks. *Comput Electr Eng* 2015; 43: 33–47.
12. Zhang J, Chen C and Cohen R. Trust modeling for message relay control and local action decision making in VANETs. *Secur Commun Netw* 2013; 6: 1–14.

13. Zhou A, Li J, Sun Q, et al. A security authentication method based on trust evaluation in VANETs. *EURASIP J Wirel Commun Netw* 2015; 2015: 59.
14. Ltifi A, Zouinkhi A and Bouhlel MS. A cooperative trust management system for VANET integrating WSN technology. *Int J Inf Netw Secur* 2013; 2: 392.
15. Li X, Liu J, Li X, et al. RGTE: a reputation-based global trust establishment in VANETs. In: *2013 5th International Conference on Intelligent Networking and Collaborative Systems*, Xi'an, China, 9–11 September 2013, pp.210–214. New York: IEEE.
16. Kumar N and Chilamkurti N. Collaborative trust aware intelligent intrusion detection in VANETs. *Comput Electr Eng* 2014; 40: 1981–1996.
17. Chen Y-M and Wei Y-C. A beacon-based trust management system for enhancing user centric location privacy in VANETs. *J Commun Netw* 2013; 15: 153–163.
18. Shaikh RA and Alzahrani AS. Intrusion-aware trust model for vehicular ad hoc networks. *Secur Commun Netw* 2014; 7: 1652–1669.
19. Huang Z, Ruj S, Cavenaghi MA, et al. A social network approach to trust management in VANETs. *Peer Peer Netw Appl* 2014; 7: 229–242.
20. Gurung S, Lin D, Squicciarini A, et al. Information-oriented trustworthiness evaluation in vehicular ad-hoc networks. In: *International conference on network and system security*, Madrid, 3–4 June 2013, pp.94–108. Berlin: Springer.
21. Zhang J, Cui J, Zhong H, et al. PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. *IEEE Trans Dependable Secure Comput*. Epub ahead of print 11 March 2019. DOI: 10.1109/TDSC.2019.2904274.
22. Alam M, Ferreira J and Fonseca J. *Intelligent transportation systems: dependable vehicular communications for improved road safety*. Berlin: Springer, 2016.
23. ETSI EN 302 637-3 V1.3.0:2018. Intelligent transport systems (ITS); vehicular communications; basic set of applications.
24. Jaeger A. *Weather hazard warning application in car-to-X communication: concepts, implementations, and evaluations*. Berlin: Springer, 2016.
25. Soleymani SA, Abdullah AH, Zareei M, et al. A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing. *IEEE Access* 2017; 5: 15619–15629.
26. Wang Y, Duan X, Tian D, et al. Throughput and delay limits of 802.11 p and its influence on highway capacity. *Proc Soc Behav Sci* 2013; 96: 2096–2104.
27. Sampson J. Traffic flow variations in urban areas. In: *2017 Southern African transport conference*, Pretoria, South Africa, 10–13 July 2017.
28. Rapaport L. Car crash death rates highest in remotest rural areas, https://www.reuters.com/article/us-health-rural-autos-crash/car-crash-death-rates-highest-in-remotest-rural-areas-idUSKBN1CA2EW (2017, accessed 23 May 2019).
29. Champahom T, Jomnonkwao S, Watthanaklang D, et al. Applying hierarchical logistic models to compare urban and rural roadway modeling of severity of rear-end vehicular crashes. *Accid Anal Prev* 2020; 141: 105537.
30. Shrira I and Noguchi K. Traffic fatalities of drivers who visit urban and rural areas: an exploratory study. *Transp Res Part F Traffic Psychol Behav* 2016; 41: 74–79.
31. Azagba S, Shan L and Latham K. Rural-urban differences in cannabis detected in fatally injured drivers in the United States. *Prev Med* 2020; 132: 105975.
32. Mahima SK, Srivastava DK, Kharya P, et al. Analysis of risk factors contributing to road traffic accidents in a tertiary care hospital: a hospital based cross-sectional study. *Chin J Traumatol* 2020; 23: 159–162.
33. Li A, Shen S, Nwosu A, et al. Investigating traffic fatality trends and restraint use among rear-seat passengers in the United States, 2000–2016. *J Saf Res* 2020; 73: 9–16.
34. Shaikh RA. Fuzzy risk-based decision method for vehicular Ad Hoc networks. *Int J Adv Comput Sci Appl* 2016; 7: 54–62.
35. Bae S. JavaScript objects. In: Bae S (ed.) *JavaScript data structures and algorithms*. Berlin: Springer, 2019, pp.83–88.
36. Veins. Open source vehicular network simulation framework, https://veins.car2x.org (2011, accessed 10 January 2019).
37. OMNeT++. Discrete event simulator, https://omnetpp.org (2019, accessed 10 January 2019).
38. SUMO. Simulation of urban mobility, http://sumo.sourceforge.net (2019, accessed 7 June 2019).
39. OpenStreetMap Foundation. OpenStreetMap, http://openstreetmap.org (2019, accessed 24 July 2019).
40. Ahmed SA, Ariffin SH and Fisal N. Overview of wireless access in vehicular environment (WAVE) protocols and standards. *Environment* 2013; 7: 8.
41. The ITS Standards Program. Fact sheets, https://www.standards.its.dot.gov/Factsheets/Factsheet/80 (2009, accessed 15 July 2019).
42. Draper AM and Weissburg MJ. Impacts of global warming and elevated CO_2 on sensory behavior in predator-prey interactions: a review and synthesis. *Front Ecol Evol* 2019; 7: 72.
43. Wu XR, Li YP, Tu SX, et al. Elevated atmospheric CO_2 might increase the health risk of long-term ingestion of leafy vegetables cultivated in residual DDT polluted soil. *Chemosphere* 2019; 227: 289–298.
44. Gu Q, Cai Z and Zhu L. Classification of imbalanced data sets by using the hybrid re-sampling algorithm based on isomap. In: *International symposium on intelligence computation and applications*, Huangshi, China, 23–25 October 2009, pp.287–296. Berlin: Springer.
45. Yao X, Zhang X, Ning H, et al. Using trust model to ensure reliable data acquisition in VANETs. *Ad Hoc Networks* 2017; 55: 107–118.
46. Oxford University Press. Oxford English dictionary, https://en.oxforddictionaries.com (2019, accessed 20 July 2019).
47. Tangade SS and Manvi SS. A survey on attacks, security and trust management solutions in VANETs. In: *2013 Fourth international conference on computing, communications and networking technologies (ICCCNT)*, Tiruchengode, India, 4–6 July 2013, pp.1–6. New York: IEEE.

48. Kavita NB and Singh RP. A hybrid approach to increase the scalability in VANETs. *Int J Appl Eng Res* 2017; 12: 5729–5738.
49. Singh E. Mobility and scalability management issues in VANET. *Int J Adv Res Sci Eng* 2018; 7: 151–155.
50. Alriyami Q, Adnane A and Smith AK. Evaluation criteria for trust management in vehicular ad-hoc networks (VANETs). In: *2014 International conference on connected vehicles and expo (ICCVE)*, Vienna, 3–7 November 2014, pp.118–123. New York: IEEE.