future internet

MDPI

Article

A New Scheme for Detecting Malicious Nodes in Vehicular Ad Hoc Networks Based on Monitoring Node Behavior

Muhsen Alkhalidy [1], Atalla Fahed Al-Serhan [2], Ayoub Alsarhan [3,*] and Bashar Igried [1]

[1] Department of Computer Science and Applications, Faculty of Prince Al-Hussein Bin Abdallah II for Information Technology, The Hashemite University, Zarqa 13133, Jordan; muhsen@hu.edu.jo (M.A.); bashar.igried@hu.edu.jo (B.I.)
[2] Department of Business Administration, Al-Bayt University, Al-Mafraq 25113, Jordan; ar_alserhan@aabu.edu.jo
[3] Department of Information Technology, Faculty of Prince Al-Hussein Bin Abdallah II for Information Technology, The Hashemite University, Zarqa 13133, Jordan
* Correspondence: ayoubm@hu.edu.jo

Abstract: Vehicular ad hoc networks have played a key role in intelligent transportation systems that considerably improve road safety and management. This new technology allows vehicles to communicate and share road information. However, malicious users may inject false emergency alerts into vehicular ad hoc networks, preventing nodes from accessing accurate road information. In order to assure the reliability and trustworthiness of information through the networks, assessing the credibility of nodes has become a critical task in vehicular ad hoc networks. A new scheme for malicious node detection is proposed in this work. Multiple factors are fed into a fuzzy logic model for evaluating the trust for each node. Vehicles are divided into clusters in our approach, and a road side unit manages each cluster. The road side unit assesses the credibility of nodes before accessing vehicular ad hoc networks. The road side unit evicts a malicious node based on trust value. Simulations are used to validate our technique. We demonstrate that our scheme can detect and evict all malicious nodes in the vehicular ad hoc network over time, lowering the ratio of malicious nodes. Furthermore, it has a positive impact on selfish node participation. The scheme increases the success rate of delivered data to the same level as the ideal cases when no selfish node is present.

Keywords: vehicular ad hoc networks; road safety; fuzzy logic

Citation: Alkhalidy, M.; Al-Serhan, A.F.; Alsarhan, A.; Igried, B. A New Scheme for Detecting Malicious Nodes in Vehicular Ad Hoc Networks Based on Monitoring Node Behavior. *Future Internet* **2022**, *14*, 223. https://doi.org/10.3390/fi14080223

Academic Editor: Ming-Chin Chuang

Received: 1 June 2022
Accepted: 18 July 2022
Published: 26 July 2022

1. Introduction

Presently, smart cities are turning into innovation hubs by leveraging cutting-edge technology. New services can be supported in these cities because of the existence of connected infrastructure and layers of intelligence that enable adapting, learning, and responding to inhabitants' needs [1–6]. However, enhancing road safety is a critical concern for developing intelligent cities where vehicles are distributed in large street networks [5,6]. Fortunately, these vehicles can share safety information continuously. In smart cities, smart driving assistance systems based on vehicular ad hoc networks (VANETs) are used to broadcast data regarding road safety information. Road information is sensitive data; therefore, exchanging traffic information via VANETs must be complete and trustworthy [7]. Concerns about security and veracity remain the principal barriers for adopting VANETs to improve road safety [6,7]. Malicious nodes can inject false information into the VANET, including bogus traffic incidents [6,7].

In VANETs, node communication has greatly improved road safety in large-scale street networks. Smart vehicles communicate, collaborate, coordinate, and share road information and resources to develop smart roads [5,6]. Security and truthfulness are then required to make such interactions via VANETs effective [4–7]. Node trust measures a node's ability to behave correctly and actually accomplish what it is supposed to do [7].

Network throughput is dramatically reduced when compromised nodes attempt to corrupt data in VANETs [5,6]. A novel incentive scheme that detects and excludes malicious nodes is proposed in this work to address this issue.

In our scheme, parameters are collected by the road side unit (RSU) to compute the trust value for each node. Collecting reliable information enables the RSU to evaluate node trust accurately. The RSU, on the other hand, is responsible for collecting data from all nodes, including other RSUs. Unfortunately, measuring trust based on an interaction between an RSU and a node is insufficient. The RSU may receive inaccurate information from a node, even if the node provides the certified reputation. Nonreliable information would affect the ultimate trust value. Eventually, the nodes' impression of their surrounding nodes would be inaccurate.

The remaining sections of this article are structured as follows: Section 1 introduces relevant work and our contributions to the study. Following that, the VANET will be discussed in Section 2. In Section 3, we describe the proposed security system. Then, in Section 4, we will provide some of the performed tests and prove the performance of the VANET under various scenarios using our method. Section 5 represents the conclusion of the article.

2. Related Work

VANETs have recently been deployed to increase road safety and traffic control efficiency. Vehicles collaborate in VANETs to communicate warning messages and road conditions, considerably improving road safety.

In [7], a new architecture was proposed to mitigate many VANET attacks while maintaining data privacy and security. The suggested architecture uses timestamps and hashing techniques to keep the messages transmitted fresh. The trustworthiness of any node that injects false data into the VANET will be reduced significantly. In [8], the authors proposed a trust-based framework that allows users to ignore false messages from misbehaving nodes. A reputation system for platoon head vehicles is developed, in which data are collected from the VANET's nodes, and an iterative filtering technique is used to reject false feedback from misbehaving nodes. A new VANET antiattack trust scheme was introduced in [9], where nodes can use it to evaluate the trustworthiness of new nodes in VANETs. Bayesian inference is used to calculate the node's local trust based on the node's previous interactions. After that, a small group of seed nodes is selected to evaluate the global trust of all the nodes in the VANET. In [10], the proposed security system uses a Software-Defined Vehicular Network to develop a trust management architecture for VANETs. Specifically, trust between vehicles and trust between nodes and infrastructure are used to model and evaluate the trustworthiness of the node.

The authors proposed an AI-enabled trust management system (AIT) in [11] to address the security challenges for VANETs. Nearby vehicles validate each message in the VANET using deep learning algorithms. The RSU excludes untrustworthy vehicles after validating the node's authenticity using the blockchain technique. A novel security paradigm was proposed in [12] to enable vehicles to judge whether data are trustworthy. Furthermore, the Pretty Good Privacy (PGP) framework handles the certificates and associated trust level.

The authors proposed a new authentication scheme for cluster-based VANETs in [13]. Nodes in VANETs are divided into clusters, and the trust degree is computed for selecting the cluster head. The sender digitally signs the messages, which are then encrypted using a public/private key provided by a trustworthy authority and decrypted by the receiver. The authors in [14] proposed a new trust-based security scheme for securing message exchange in a VANET. The VANET Grouping Algorithm (VGA) was presented to group nodes into clusters and elect cluster heads. After dividing the VANET into clusters, a trust management scheme is used to evaluate the reputations of vehicles. In [15], a new trust management-based scheme was proposed. The trust degree for each node is computed for authentication purpose. The authors in [16] described a new framework for efficiently delivering messages between vehicles and RSUs. Blockchain technology is adopted in

the proposed framework to support data integrity, traceability, and reliability features that traditional reputation systems fail to provide. In [17], the authors suggested a novel dynamic entity-centric trust model. Trust is calculated based on weight dependence, the type of applications, and node authority levels. The results showed that the proposed trust model improves the security of the GPSR routing protocol with minimal delay and increases the success rate of data delivery.

The authors in [18] proposed a new trust management system based on federated learning. The trust level for each node is computed firstly to improve the accuracy of the collected data. A state-of-the-art protocol was proposed in [19] for securing communication in VANETs. Elliptic curve cryptography is adopted in the proposed system to assure communication security at no additional expense. Policy rules were used in [20] to assess the trustworthiness of data and IoT devices in smart cities based on reporting history and data context. In [20], the authors proposed a new approach based on game theory for detecting malicious nodes in VANETs.

Therefore, unlike other solutions, we propose a new, adaptive, trust-based security scheme where the trust for each node is computed based on feedback from other nodes, data accuracy, and direct trust between the node and RSU. Vehicles play a vital role in our data interaction scheme. Because our scheme not only uses the RSU to calculate and share the trust value, but also considers how vehicles calculate trust, this structure is flexible enough to solve the problem of low accuracy and real-time trust information that a vehicle may face when calculating trust. The scheme is scalable where the nodes are divided into scalable clusters. To mitigate the effect of malicious nodes and improve road safety, these nodes are evicted from the VANET using our scheme. Our scheme can be adopted for road safety, and no extra infrastructure is required. Our scheme can benefit a wide range of new road safety and driver assistance applications.

3. Network Overview

In our work, each section (i.e., cluster) of the road is broken down into K sections. The RSU manages the nodes and communication in a cluster for each segment. Each node is equipped with one IEEE 802.11b-based transceiver. The spectrum is divided into channels that do not overlap (16 channels per RSU separated by 5 MHZ), with transmission and power mask restrictions comparable to the ISM band.

Each vehicle has radio communication equipment, and the RSU that operates as a relay point for other nodes. Moving vehicles are connected using statically deployed access points or base stations (RSUs). Connecting vehicles to RSUs enables more precise and efficient traffic control, thereby significantly lowering traffic congestion, accidents, and pollution. Vehicles have onboard sensors. A GPS receiver, speedometer, accelerometer, and digital map are among the sensors that help a vehicle gather road data. The road condition is sensed by each node in the cluster and reported to the RSU. In order to protect the lives of drivers on the road, the RSU transmits emergency safety alerts to all vehicles after collecting and evaluating road data. Each vehicle is assumed to be inside the range of the i^{th} RSU if and only if the following condition is met:

$$S_j^i \geq \delta \tag{1}$$

where S_j^i is the signal power received at the i^{th} RSU from the j^{th} node, and δ is the threshold for signal power. Signal power is computed as described in [21]. A large number of RSUs are distributed over the street. The RSU is responsible for the management of all vehicles registered in its segment. Each vehicle is managed with exactly one RSU. Each node has a unique ID, which can be the MAC address of the node. We secure the safety messages transmitted between network nodes by encrypting them with symmetric key cryptography. The node has private and public cryptographic keys, a certificate issued by the RSU. The j^{th} node selects the i^{th} RSU for coordination that has the strongest signal as follows:

$$R_j^i = S_j^i \tag{2}$$

where R is the set of RSUs in the street. The i^{th} RSU (cluster head) maintains a list of its nodes L_i. L_i is broadcast to all cluster members.

Vehicles in our work move at random and vary their speed at will. At each road intersection, vehicles choose a way at random. When a vehicle selects a direction at an intersection, it proceeds straight until it reaches the next intersection where it can change direction. Figure 1. illustrates the architecture of VANET.

Definition 1. *VANET can be represented as a network graph* $G_1 = (V_1, E_1)$, *where* $V_1 = (v_1, v_2, \ldots, v_n)$ *and is a collection of n nodes, comprising vehicles and RSUs, and* $E_1 = \{(i, j) : i, j \in V_1\}$ *and is the set of links.*

Definition 2. *In our model, the graph G is utilized to represent the city's roads.* $G_2 = (V_2, E_2)$ *and is a graph made up of edge set* E_2 *and vertex set* V_2. *The road over intersections* v_i *and* v_j *is represented by the edge* $e_{i,j}$. *The driver can drive directly from intersection* v_i *to intersection* v_j. *We call* $e_{i,j}$ *a link, and a road is the undirected path that connects vertex* v_i *with vertex* v_j.

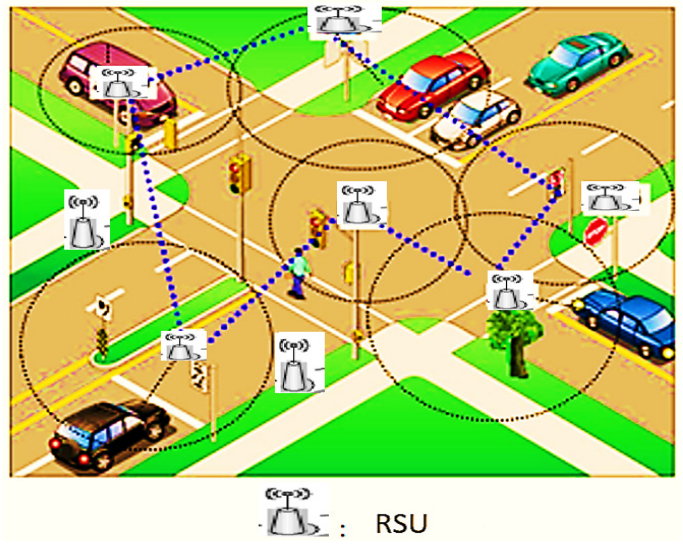

Figure 1. Architecture of VANET.

4. Trust Evaluation in VANET

This section defines the communication messages the nodes exchange in VANET during the trust computation model and the system constraints.

Definition 3. *A message in VANET is a tuple* $\langle \alpha, X, Y, C, T \rangle$ *where* α *indicates the message type, whether it is a request or provides a service in VANET;* X, Y *are sender and receiver of message, respectively;* C *is the message, and* T *is the message delivery time.*

Assume W_i is the set of trustworthy nodes that was managed by the i^{th} RSU. W_i is changing continuously based on environmental conditions. The RSU may request information or service from a trustworthy j^{th} node by sending a message. After that, the j^{th} node either refuses to collaborate, is obligated to serve, or accepts the request. The RSU excludes a node if it refuses collaboration and sends a message about node exclusion to all its cluster members. After receiving the exclusion message, each node looks up its cluster members' table entry and deletes the malicious node.

Meanwhile, the RSU may consult other RSUs and trustworthy nodes to accept new nodes in VANET. The requested referee has three options for responding: offering the node's trust level, excusing due to a lack of information, or refusing to reveal information about the node. Any referee would be penalized by the RSU for inaccurate information,

which will not be considered for future consultation. As a result, providing the right trust level is preferable to hiding it if the referee is dissatisfied with the node's behavior.

4.1. Trust Level Computatiion

The problem of trust computation for nodes in VANET can be formalized as follows:

Definition 4 *Let N be a set of nodes in VANET and T_l a set of accepted values of trust levels. The trust function F_T maps the node from N to a value from the domain T_l as follows:*

$$F_T(j) = \{T_l,\ 0 < T_l \leq 1\ 0,\ O.W\ \} \tag{3}$$

In our work, each event in VANET takes two values: 1 means positive evidence, and a 0 value means bad evidence. Assume B is a random variable representing the events performed by a node in VANET. The Bernoulli distribution is a discrete distribution [22,23] with two possible outcomes denoted by b = 0 and b = 1, with b = 1 ("positive") occurring with probability p and b = 0 ("bad") occurring with probability 1-p, where $0 < p < 1$ [22,23]. As a result, it has a probability density function, which can be written as [22,23]:

$$P(b) = \{1 - p,\ b = 0\ p,\ b = 1\ \} \tag{4}$$

This function can be written as follows [22,23]:

$$(b,\ p) = p^b(1-p)^{1-b},\ \mathrm{b} \in \{0,1\} \tag{5}$$

where p is the probability that the evidence is positive. The variable B follows a Bernoulli distribution $b(1,\ p)$. E(B) is the expectation of the variable B, and it can be written as follows [22,23]:

$$\mathrm{E}(B) = p \tag{6}$$

$$\mathrm{V}(B) = p(1-p) \tag{7}$$

The corresponding variance is:

Central Limit Theorem (CLT) and the law of large numbers predict that the mean of all variables selected from the same population will be nearly equal to the population's mean, given a big enough sample size from the population with finite variance. As the sample size increases, the variances of these samples tend to match those of the population as a whole, according to the Law of Large Numbers. The random variable B is the weighted average of n independent events that are performed by the i^{th} node. The events follow the same distribution and are independent because the probability that the event is positive is independent of the probability that the next event is positive. In our model, the following criteria will be considered for computing the trust level for a node in VANET:

- Recommendations from other nodes, including other RSUs.
- Direct trust.
- Accuracy of the information provided.

4.1.1. Recommendations from Other Nodes

The RSU informs the referees to report on the credibility of the j^{th} node to allow it to communicate data with others. Referees send their recommendations based on their previous interactions with the j^{th} node. However, a referee may excuse if it does not interact directly with the j^{th} node. The RSU considers only a referee's recommendation if the number of contacts with the j^{th} node exceeds threshold β. The set of referees whose recommendations are taken into account for evaluating the trustworthiness of the j^{th} node can be expressed as follows:

$$R = \left\{i,\ a_j^i > \beta\right\} \tag{8}$$

where a_j^i is the number of contacts between the i^{th} node and j^{th} node. This condition promotes recommendations from nodes with a longer history of contact with the j^{th} node. The recommendation of the i^h node is computed as follows:

$$C_j^i = \frac{G_j^i}{a_j^i} \tag{9}$$

where G_j^i is the number of positive interactions between the j^{th} and i^{th} nodes.

4.1.2. Direct Trust

The RSU computes the trust level of each new node based on their previous direct interactions. In our work, the RSU evaluates its interactions with the j^{th} node according to a scale of n levels numbered from 1 (the largest successful interaction) to n (the lowest successful interaction). We assumed $a_j^i(t)$ is the number of interactions of type t between the i^{th} RSU and the j^{th} node. The RSU computes the trust for the j^{th} node as follows:

$$S(j) = \frac{\sum_{x=1}^{m} w_x \sum_{h=1}^{a_j^i(x)} v_h}{\sum_{x=1}^{m} a_j^i(x)} \tag{10}$$

where w_x denotes the importance of the completed transaction, and v_h reflects the degree of cooperation of the j^{th} node with the RSU. The RSU must distinguish between transactions carried out by the j^{th} node. Transactions of the same type have varying values in our work, reflecting each transaction's importance. This value is represented by v_h.

4.1.3. Accuracy of the Information Provided

The RSU constantly checks the correctness and accuracy of information produced by nodes in VANET. This is because the VANET environment is dynamic and subject to rapid change. The objective is to use VANET to spread accurate information and deal with misleading safety signals. When calculating the node's trust, the degree of message accuracy could be represented as a coefficient. The Hamming distance [24] will be employed in our research to assess the accuracy of information provided by a node. The information provided by the j^{th} node is compared to the information provided by the most trustworthy node. The most trusted node is chosen by the i^{th} RSU as follows:

$$V = S(j) \tag{11}$$

The evaluation value of the Hamming distance h_d^j can be evaluated as follows:

$$\hat{h}_d^j = \frac{h_d^j}{L(M)} \tag{12}$$

where $L(M)$ denotes the length of the message (i.e., total number of bits) to be checked.

4.1.4. Fuzzy Integral for Trust Level Computation

Machine learning has been successfully applied to a wide range of applications in recent years, such as security problems [25–28]. Trust evaluation for each node aims to create a secure VANET that can significantly improve road safety. RSUs make independent decisions for selecting nodes that can exchange data over VANET. Fuzzy integral logic is adopted in our work to extract the final trust level for each node. Assume the set $\Lambda = \{t_1, t_2, t_3, ..., t_n\}$ indicates the possibilities or solutions from which the RSU must select (i.e., trust level for a node). Let $\psi = \{a_1, a_2, a_3, ..., a_n\}$ represent the limited set of criteria that must be considered while calculating a node's trust value.

Each node is associated with a vector $\Lambda_i \in \Lambda$ whose components $t_i \in \psi$, t_i reflect the value of the i^{th} characteristic that will be considered in calculating trustworthiness. There would be an objective function for each of the criteria. A utility function is used to simulate the selection process preferences η based on these criteria:

$$O : \Lambda \rightarrow \text{I.R} \tag{13}$$

Such that:

$$\forall \text{ a, b} \in \eta, \text{ a } \eta \text{ b} \Leftrightarrow \text{O (a)} \geq \text{O (b)} \tag{14}$$

The utility functions that are labelled $O_1(t_1), \ldots, O_n(t_n)$ transfer each criterion of the j^{th} node to a single satisfaction scale $\varepsilon \in$ I.R. Each node's criteria must be combined into a single score or ranking for the j^{th} node, as follows:

$$\forall\, t_i \,, \text{O}\,(t_i\,) = H((O_1\ (t_1), \ldots O_n\ (t_n)) \tag{15}$$

λ-fuzzy measure [29] is used in our work to compute the overall trust evaluation for the j^{th} node.

5. Performance Evaluation

The performance of our scheme was evaluated by examining its ability to recognize untrustworthy nodes and evict malicious nodes from the network. The main concern of our scheme is increasing the received ratio of accurate data and reducing the ratio of corrupted data. The simulation model was built using MatLab. The key performance measures of interest in the simulations are:

1. Throughput is the average rate at which a message is delivered successfully via a communication link.
2. Spectrum utilization is the average amount of time the spectrum is kept busy. The utilization is calculated as follows:

$$U = \frac{T_u}{T_s} \tag{16}$$

where T_s is the simulation duration, and T_u is the length of time the spectrum is kept busy. The findings were then averaged across a sufficient number of independent runs to ensure that the confidence level is at least 95% and that the relative errors do not exceed 5%. In this section, we analyzed the performance using a variety of parameter values. Table 1 shows the parameters used to evaluate the proposed scheme. The input parameters' values were selected to reflect a portion of the reality of wireless applications, such as phone call traffic.

Malicious nodes keep sending false messages and altering some of them while forwarding a received message. Furthermore, some nodes reject relaying some messages. Our scheme tries to exclude such nodes. As shown in Figure 2, our security scheme (secured VANET, (SV)) produced better throughput outcomes in the simulations than a VANET without any security mechanisms (UV). The figure displays the effect of varying load on the reported throughput for the SV and the UV schemes. The figure shows that the proposed SV scheme consistently outperforms UV since it excludes malicious nodes from VANET and reduces their number to the lowest possible number. Therefore, the reported throughput for SV shifts to a higher level for different traffic values. Sometimes, malicious nodes reject forwarding packets. Fortunately, nodes that continue to send false warnings to keep the spectrum busy are excluded from the system using our scheme. Besides utilizing the recommendation from other nodes, the RSU uses its experience to evaluate untrustworthy nodes and evict them from VANET. The malicious node evection ratio is plotted in Figure 3. It can be observed that the evection ratio increases as the number of malicious nodes increases.

Table 1. Simulation Parameters.

Parameter		Value
Number of messages per MC		Random
Type of interface per node		802.11 b
MAC layer		IEEE 802.11 b
Transmission power		0.1 watt
Packet size		512
Transmission range		250–500
Channel		Wireless channel
Max vehicle speed		110 km/h
Warning message cycle		100 ms
Simulation Device	Intel i5 Core	2.50 GHz
	Process cores	2 × 2.50 GHz
	RAM	6 GB
	OS	Windows 7 64 bit

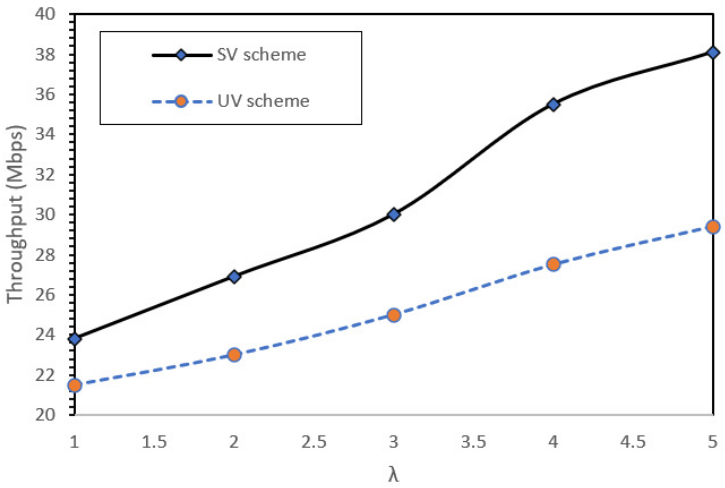

Figure 2. Throughput at various arrival rates for requests.

The attackers might continue sending the RSU false reports to gain exclusive access to the spectrum and prevent other nodes from accessing it. The utilization of resources is realized under the premise of the preceding experimental scenario and trust model. Spectrum utilization results are displayed in Figure 4. Clearly, the utilization decreases significantly as the percentage of malicious nodes increases. Fortunately, the figure shows that our scheme effectively utilizes the spectrum even when the percentage of attackers increases considerably. The SV scheme evicts misbehaving nodes that result in inefficient spectrum usage. However, the UV scheme's utilization reduces considerably as the percentage of malicious nodes increases. Because it cannot cope with malicious nodes, the UV fails to make effective spectrum use.

In Figure 5, the average delay is plotted against various percentages of attackers. It can be shown that as the number of malicious nodes increases, the average delay increases. Attackers send dummy messages to keep the spectrum busy and reserve VANET resources. As a result, users will be unable to access the spectrum, resulting in a considerable increase in delay. Untrustworthy nodes that refuse to relay or drop packets are ejected from VANET using our scheme. The results in Figure 5 demonstrate our scheme's ability to decrease the delay in various system settings. In addition, to reject false alarms from untrustworthy

nodes, the RSU notifies trustworthy nodes to avoid connecting with these nodes. In any scenario, our scheme prevents untrustworthy nodes from accessing the spectrum.

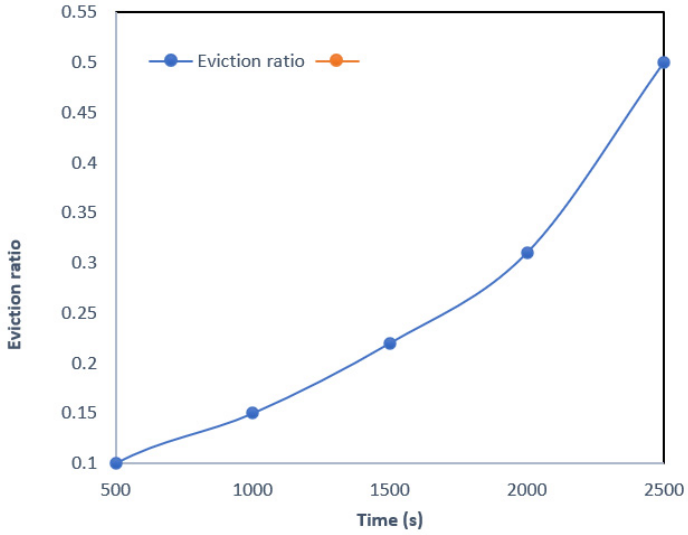

Figure 3. Eviction ratio at different simulation run times.

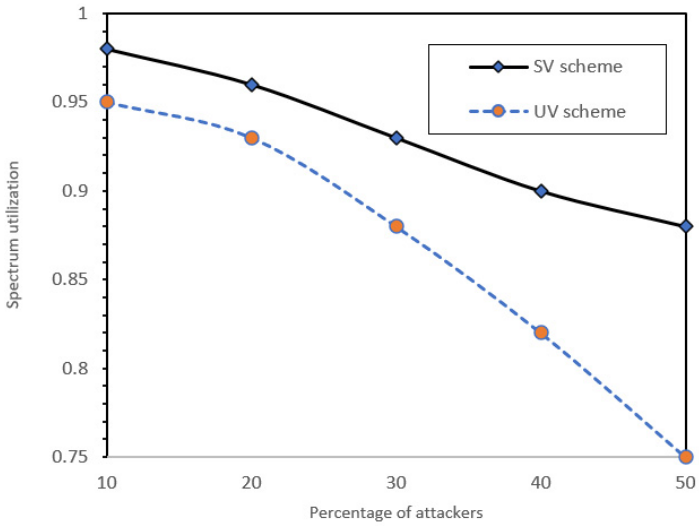

Figure 4. Comparison of utilization under various percentages of attackers.

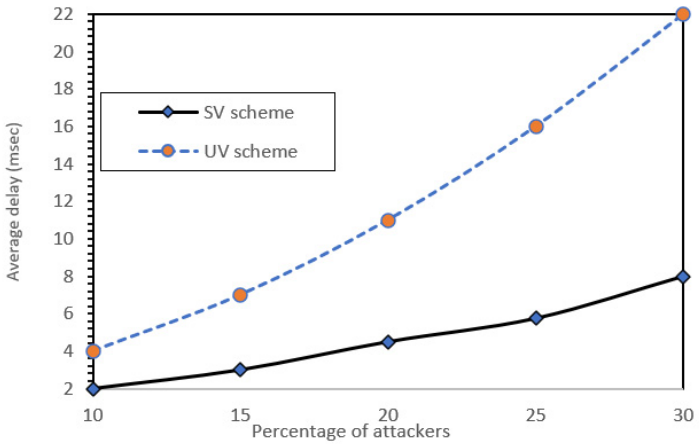

Figure 5. Comparison of the two schemes' delay.

6. Conclusions and Future Work

It is critical to secure VANET communication to save lives. VANET aims to ensure safe driving by assisting drivers in recognizing risks and improving road safety and traffic conditions. Adversary nodes may launch a variety of attacks in VANET. These attacks have a substantial impact on VANET's performance and reliability. As a result, this research introduces a novel trust model for identifying and excluding attacker nodes in a VANET by monitoring node activity. It is based on a fuzzy logic model. Several criteria are fed into the model to calculate the final value of trust. Our scheme provides a practical solution for dealing with malicious and selfish nodes in VANETs without needing additional VANET components. When malicious nodes have a low trust value, the scheme evicts them from VANET.

Furthermore, evicting any selfish node encourages selfish nodes to collaborate. Through simulations, we demonstrated that our scheme could detect and evict all malicious nodes from the VANET while simultaneously increasing throughput and minimizing delay. Our solution encourages all nodes to participate in providing accurate information without being self-serving. We want to use a verification tool in the future to ensure that our scheme is robust to various attacks and that it only selects the most trustworthy nodes in the VANET. Furthermore, we would like to conduct a similar analysis on a real-world system.

Author Contributions: Conceptualization, M.A.; Formal analysis, A.F.A.-S.; Investigation, A.F.A.-S.; and B.I.; Methodology, M.A., A.A. and B.I.; Software, A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zeadally, S.; Hunt, R.; Chen, Y.S.; Irwin, A.; Hassan, A. Vehicular ad hoc networks (VANETS): Status, results, and challenges. *Telecommun. Syst.* **2012**, *50*, 217–241. [CrossRef]
2. Wang, Y.; Ding, Y.; Wu, Q.; Wei, Y.; Qin, B.; Wang, H. Privacy-Preserving Cloud-Based Road Condition Monitoring with Source Authentication in VANETs. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 1779–1790. [CrossRef]
3. Mishra, R.; Singh, A.; Kumar, R. VANET security: Issues, challenges and solutions. In Proceedings of the International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 3–5 March 2016.
4. Shankar, R.; Singh, A.V. Use of VANETs for human Safety in road transportation. In Proceedings of the International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), Noida, India, 2–4 September 2015.
5. Upadhyaya, A.N.; Shah, J.S. Attacks on vanet security. *Int. J. Comput. Eng. Technol.* **2018**, *9*, 8–19.
6. Padmavathi, K.; Maneendhar, R. A Surveying on Road Safety Using Vehicular Communication Networks. *J. Comput. Appl.* **2012**, *5*, 460–465.
7. Khan, A.S.; Balan, K.; Javed, Y.; Tarmizi, S.; Abdullah, J. Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. *Sensors* **2019**, *19*, 4954. [CrossRef] [PubMed]
8. Hu, H.; Lu, R.; Zhang, Z.; Shao, J. REPLACE: A Reliable Trust-Based Platoon Service Recommendation Scheme in VANET. *IEEE Trans. Veh. Technol.* **2017**, *66*, 1786–1797. [CrossRef]
9. Zhang, A.J.; Zheng, K.; Zhang, D.; Yan, B. AATMS: An Anti-Attack Trust Management Scheme in VANET. *IEEE Access* **2020**, *8*, 21077–21090. [CrossRef]
10. Ming, M.; Peng, Y.; Tao, H.; Zhen, Z.; Xiangyu, L.; Jingwei, L.; Vishal, S. Hierarchical Hybrid Trust Management Scheme in SDN-Enabled VANETs. *Mob. Inf. Syst.* **2021**, *2021*, 7611619.
11. Zhang, C.; Li, W.; Luo, Y.; Hu, Y. AIT: An AI-Enabled Trust Management System for Vehicular Networks Using Blockchain Technology. *Internet Things J. IEEE* **2021**, *8*, 3157–3169. [CrossRef]
12. Madl, T. Security Concept with Distributed Trust-Levels for Autonomous Cooperative Vehicle Networks. In Proceedings of the IEEE Intelligent Vehicles Symposium (IV), Nagoya, Japan, 1–17 July 2021.
13. Sugumar, R.; Rengarajan, A.; Jayakumar, C. Trust based authentication technique for cluster based vehicular ad hoc networks (VANET). *Wirel. Netw.* **2018**, *24*, 373–382. [CrossRef]
14. Abassi, R.; Ben Chehida Douss, A.; Sauveron, D. TSME: A trust-based security scheme for message exchange in vehicular Ad hoc networks. *Hum.-Cent. Comput. Inf. Sci.* **2020**, *10*, 43. [CrossRef]
15. Awan, K.A.; Din, I.U.; Almogren, A.; Kim, B.-S.; Altameem, A. vTrust: An IoT-Enabled Trust-Based Secure Wireless Energy Sharing Mechanism for Vehicular Ad Hoc Networks. *Sensors* **2021**, *21*, 7363. [CrossRef] [PubMed]

16. Vintimilla-Tapia, P.; Bravo-Torres, J.; López-Nores, M.; Gallegos-Segovia, P.; Ordóñez-Morales, E.; Ramos-Cabrer, M. VaNetChain: A Framework for Trustworthy Exchanges of Information in VANETs Based on Blockchain and a Virtualization Layer. *Appl. Sci.* **2020**, *10*, 7930. [CrossRef]
17. Yao, X.; Zhang, X.; Ning, H.; Li, P. Using trust model to ensure reliable data acquisition in VANETs. *Ad Hoc Netw.* **2017**, *55*, 107–118. [CrossRef]
18. Haddaji, A.; Ayed, S.; Chaari, L. Federated Learning with Blockchain Approach for Trust Management in IoV. In Proceedings of the International Conference on Advanced Information Networking and Applications, Sydney, Australia, 13–15 April 2022; Springer: Cham, Switzerland, 2022; pp. 411–423.
19. Patel, A.; Shah, N.; Limbasiya, T.; Das, D. VehicleChain: Blockchain-based Vehicular Data Transmission Scheme for Smart City. In Proceedings of the IEEE International Conference on Systems, Man and Cybernetics (SMC), Bari, Italy, 28 November 2019.
20. Liu, Y.; Wang, Y.; Chang, G. Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2740–2749. [CrossRef]
21. Alsarhan, A.; Agarwal, A. Cluster-Based Spectrum Management Using Cognitive Radios in Wireless Mesh Network. In Proceedings of the 18th International Conference on Computer Communications and Networks, San Francisco, CA, USA, 3–6 August 2009.
22. Weisstein, E.W. "Bernoulli Distribution." From MathWorld—A Wolfram Web Resource. Available online: https://mathworld.wolfram.com/BernoulliDistribution.html (accessed on 17 July 2022).
23. Fischer, H. *A History of the Central Limit Theorem: From Classical to Modern Probability Theory*; Sources and Studies in the History of Mathematics and Physical Sciences; Springer: New York, NY, USA, 2011. [CrossRef]
24. Tzeng, G.H.; OuYang, Y.P.; Lin, C.T.; Chen, C.B. Hierarchical MADM with fuzzy integral for evaluating enterprise intranet web sites. *Inf. Sci.* **2005**, *169*, 409–426. [CrossRef]
25. Alsarhan, A.; Al-Ghuwairi, A.R.; Alshdaifat, E.; Idhaim, H. A Novel Scheme for Malicious Nodes Detection in Cloud Markets Based on Fuzzy Logic Technique. *Int. J. Interact. Mob. Technol.* **2022**, *16*, 136–150. [CrossRef]
26. Alsarhan, A.; Al-Ghuwairi, A.R.; Almalkawi, I.T.; Alauthman, M.; Al-Dubai, A. Machine learning-driven optimization for intrusion detection in smart vehicular networks. *Wirel. Pers. Commun.* **2021**, *117*, 3129–3152. [CrossRef]
27. Alsarhan, A.; Alauthman, M.; Alshdaifat, E.; Al-Ghuwairi, A.-R.; Al-Dubai, A. Machine Learning-driven optimization for SVM-based intrusion detection system in vehicular ad hoc networks. *J. Ambient. Intell. Humaniz. Comput.* **2021**, 1–10. [CrossRef]
28. Han, J.; Kamber, M.; Pei, J. *Data Mining: Concepts and Techniques*; The Morgan Kaufmann Series in Data Management Systems; Morgan Kaufmann Publishers: Waltham, MA, USA, 2011; ISBN 978-0123814791.
29. Sugeno, M. Theory of Fuzzy Integrals and Its Applications. Ph.D. Dissertation, Tokyo Institute of Technology, Tokyo, Japan, 1974.