electronics

MDPI

Article

A Privacy Preserved, Trust Relationship (PTR) Model for Internet of Vehicles

Haleem Farman [1,*,†], Abizar Khalil [1,†], Naveed Ahmad [2,*], Waleed Albattah [3], Muazzam A. Khan [4] and Muhammad Islam [5]

1 Department of Computer Science, Islamia College Peshawar, Peshawar 25120, Pakistan; abizar111@gmail.com
2 Department of Computer Science, Prince Sultan University, Riyadh 12435, Saudi Arabia
3 Department of Information Technology, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia; w.Albattah@qu.edu.sa
4 Department of Computer Science, Quaid-e-Azam University, Islamabad 45320, Pakistan; Muazzam.khattak@qau.edu.pk
5 Department of Electrical Engineering, College of Engineering and Information Technology, Unaizah Colleges, Unaizah 2053, Saudi Arabia; M.islam@oc.edu.sa
* Correspondence: haleem.farman@icp.edu.pk (H.F.); nahmed@psu.edu.sa (N.A.)
† Haleem Farman and Abizar Khalil has an equal contribution.

Abstract: The Internet of vehicles (IoV) depicts a reality where ordinary things are connected to vehicular ad-hoc networks (VANETs), allowing them to transmit and collaborate. By placing these regular objects in VANETs and making them available at any time, this network and data sharing may raise real privacy and security issues. Thus, group-based communication is mostly preferred in the literature. However, in heavy network scenarios, cluster-based communication mostly leads to additional overload in the form of the group leader that causes delay and disrupts the performance of a network. Due to the interaction of VANETs with applications that are not stable for life, privacy and security mechanism for detecting many malicious nodes is in great demand. Therefore, a multi-phantom node selection has been proposed in this paper to select trustworthy, normal, and malicious nodes. The multi-phantom node scheme is proposed to reduce the phantom node load, where the multi-lateral nodes in a cluster act as a phantom node to share the load. A multi criteria decision-making (MCDM) methodology (analytic network process) is used to optimize the phantom node to pre-serve privacy using the privacy preserved trust relationship (PTR) model. The results show checking the stability of parameters and using sensitivity analysis by considering different scenarios for the most optimal phantom node to preserve vehicle location privacy. The impact of the proposed model will be more clearly visible in its real-time implementation in urban areas vehicle networks.

Keywords: location privacy; Internet of things; Internet of vehicles; ubiquities computing; multi-criteria decision; VANETs

Citation: Farman, H.; Khalil, A.; Ahmad, N.; Albattah, W.; Khan, M.A.; Islam, M. A Privacy Preserved, Trust Relationship (PTR) Model for Internet of Vehicles. *Electronics* **2021**, *10*, 3105. https://doi.org/10.3390/electronics10243105

Academic Editors: Dongkyun Kim, Qinghe Du, Mehdi Sookhak, Lei Shu, Nurul I. Sarkar, Jemal H. Abawajy and Francisco Falcone

Received: 7 November 2021
Accepted: 2 December 2021
Published: 14 December 2021

1. Introduction

In 2001, the VANETs were first described and introduced [1] under "car-to-car-ad-hoc mobile communication applications," which enable to form networks and relay information between cars. In VANETs, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) transmission systems coexist to deliver security, safety, road protection, emergency services, infotainment, navigation, and payment service and permit the vehicles to share information. These applications allow nodes to connect with infrastructure networks, citizens, and the network, which leads VANETs to become the fundamental paradigm known as the Internet of vehicles (IoVs) [2,3]. An intelligent transport system (ITS) has emerged transportation network. It has developed into a digital, knowledge-based, and wireless-enabled superhighway [4,5], and such connectivity and sharing of information have raised severe security and privacy problems.

Privacy is still a big concern emerging from VANETs. Meanwhile, vehicles sharing thoughtful information regarding themselves and neighbor's vehicles, the risk of sensitive information leakage rises leading to privacy hinders attacks. Malevolent vehicles are entitled as intruder, adversary, malicious and rogue vehicles that execute malevolent events such that signal sniffing, pattern sniffing, altering of information of packets, dropping packets, etc. Therefore, these intruder, adversary, malicious and rogue entities from disturbing the normal network activities, numerous anomalies, signature, watchdog, cross-layer, and honeypot-based intrusion detection system (IDS) mechanisms are proposed but each has its limitations.

1.1. Motivation

Many privacy and security mechanisms are offered which titles to improve privacy and security in VANETs, but these techniques have a harmful impact on network performance. Therefore, a location privacy solution is needed that improves the privacy of VANETs but does not deteriorate network performance. The researchers offer a variety of IDS systems, but the majority of them have a highly complex approach to detecting malevolent nodes, which requires massive network resources and computing. Thus, the privacy preserved trust relationship model that offers phantom node selection, ranking the nodes' trustworthiness and maliciousness of the nodes on certain criteria, has been proposed in this work. In phantom node-based communication, the phantom node is responsible for communicating with all nodes in the network within radio range. Therefore, in crowded network situations, the phantom node can easily become overloaded by handover, takeover and can cause decision-making delays and deteriorating network performance. Therefore, a model of multiple phantom nodes has been proposed in this paper in which multiple vehicles act as phantom nodes. The analytical network process (ANP) method has been adopted to select phantom nodes in privacy preserved secure communication. Different significant parameters are considered, and each non-malevolent vehicle is allotted levels of trust. Therefore, nodes that are not malicious and have a grade equal to or higher than the certain threshold are selected as another phantom node. In literature, ANP has been used in a variety of applications such as cluster head selection in wireless sensor networks [6], source location privacy preservation [7], controller selection in software-defined networks [8], next forwarder selection in VANETs [9] and many more.

1.2. Contributions

- Different parameters criteria are suggested in V2V and V2I infrastructure to detect malevolent nodes.
- The proposed model uses the PTR trust threshold to grade the most trustworthy, normal, and malicious nodes in a network.
- The concept of handover and the multi-phantom node is proposed to improve network performance and reduce phantom node load of handover in dense network scenarios.
- A multi-criteria decision-making method is proposed to select the optimal phantom node based on several parameters.
- For the secure dissemination of information, existing trust models (entity-driven, data-oriented, and combined trust model) are used.

1.3. Handover in VANETs

Handovers in VANETs mean switching from one network point to another network point [4]. The handover management strives to ensure active connections when the mobile node shifts its attachment point. Handover is the approach used in MANETs and VANETs for improving mobility. In VANETs, vehicles communicate directly or via other relay vehicles (RVs) with roadside units (RSUs) in V2I and V2V communication modes. When a node reaches a new RSU/RV communication area, the existing RSU/RV needs handover to a new area. Handover is used to boost the ad-hoc network's quality of service (QoS).

There are three critical phases of a simple handover process: measurements, decision, and execution.

1.3.1. Measurement Phase

A mobile station can discover different wireless networks depending on broadcast services' advertisements. The mobile unit scans and produces a list of access points (APs) prioritized by the signal strength received for these messages on designated networks. The method of scanning is classified into active and passive. In active, the station will listen and send messages, while in passive scanning, the station listens only to message.

1.3.2. Decision

Once the management phase is done, next is decision making, in which the station can determine when and to whom the handover should be made.

1.3.3. Execution

The final step is to carry out the real transfer of control. The information and all contextual information about the station will be passed to the next system in the current network.

In the PTR model, a node is selected as phantom node (A), and after some time, phantom node (A) is disappeared from the network, then phantom node (B) will be the phantom node. Furthermore, if a new node joins the network, phantom node (B) will scan the network and check the threshold value; if the threshold value is higher than other nodes, then phantom node (B) will hand over the responsibility of phantom node (A) to a new phantom node as shown in Figure 1. Moreover, if the new node value is less than the threshold, a new node will be a malicious node and be removed from the network.

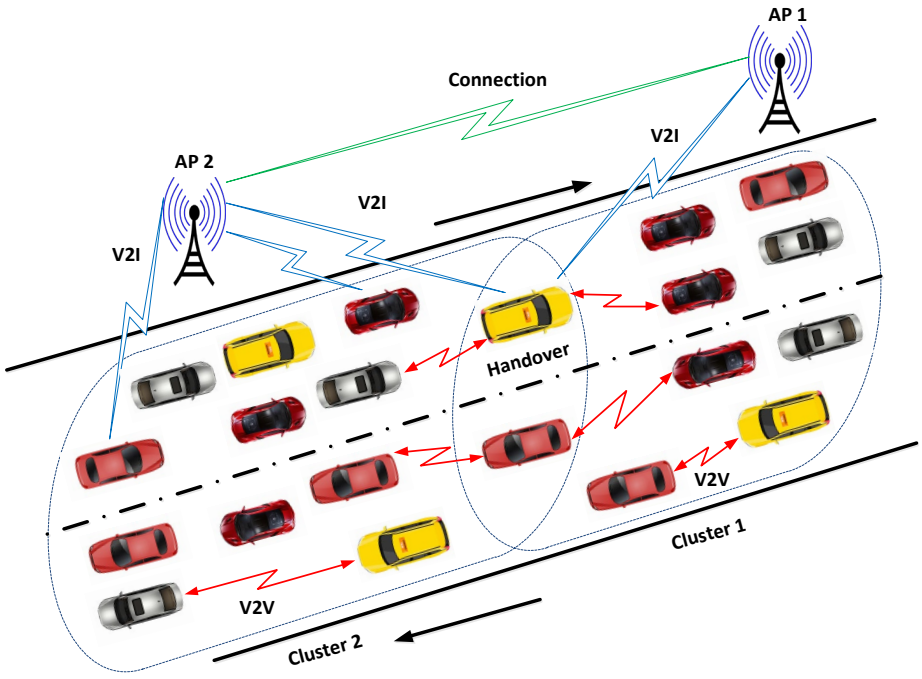

Figure 1. Handover in VANETs.

1.4. Privacy

Privacy is a state of not having undisclosed or possessed unidentified personal details [10]. Privacy is a consequence that other people do not know or have unknown personal knowledge. In the Internet of things (IoT) arena, privacy is one of the highest challenges for most users. Most of the personal drivers for the government official, businessmen, tycoons, and even for common citizens do not want to reveal their personal

location to the unknown person or any other third party services. In particular, access to personal information such as drive learning patterns, advanced knowledge of location, home and work, health, political party affiliation, social links, etc. Knowing all this information gives adversaries an easy chance to plan their operations. Although several protocols for vehicle communication have been placed within a network, IoV location privacy applications still face challenges. To address the location privacy violation issues in VANETs, sophisticated confirmation methods with a high level of traceability, auditor, trust authority, and government agencies to check and validate the data in the cloud, and tamper-proof on-board unit (OBU) device for the IoT sensors needs to be included. There are two types of privacy, one is content privacy, and the other is context privacy. We have focused on location privacy which comes under the context of privacy. Location privacy is to safeguard the user's location information [11]. We may also consider the privacy of the itinerary from the perspective of location, which defines the opportunity to protect the mobility patterns of nodes. Threats to location privacy stem from the capability of adversary vehicles that have spectrum analyzer of signals or angle of arrival of signal [12] to collect information from the observation of user communication without direct entrance to the content of the messages exchanged.

1.5. Trust Models

The term "trust" comes from the social sciences arena. Someone can infer another person's behavior based on their previous conduct. Trust building is one of the most critical aspects of the safety of any system. Trust refers to several relationships between the nodes involved in the network operations. In VANETs, the creation of trust plays a major role in preventing attacks. In VANETs, a node can measure the trustworthiness of messages it receives from other nodes. Table 1 shows different trust models that have not archived all the preferred and desire properties. It is pertinent to mention that robustness needs more attention in VANETs when it comes to life-critical applications [13].

Table 1. Trust models and their priority.

Approaches	**[14]**	**[15]**	**[16]**	**[17]**	**[18]**	**[19]**	**[20]**
Robustness	-	-	√	-	-	-	-
Privacy	-	√	√	√	-	√	-
Security	√	-	√	√	√	√	√
Confidence	√	-	-	√	√	√	-
Scalability	-	-	-	√	√	-	-
Dynamics	√	√	-	√	√	√	√
Sparsity	-	-	√	√	√	√	√
Decentralized	√	√	√	√	√	-	√

There are two kinds of trust models in VANETs, centralized and decentralized. In a centralized structure, a trust authority is responsible to calculate, compute and organize all vehicles' trust levels. While in a decentralized framework, an entity has to detect other entities previse actions, performances, activities, behavior and compute their trust level. Trust can be measured as a real number between (0, 1) or just for example (not trust, little trust, trust, very trust) and so on. Trust models are categorized into three kinds.

1.5.1. Entity Oriented Trust Model (EOTM)

A message can be trusted if issued by a trusted vehicle, which is a general characteristic of trust models based on entities. Some models are based on the roles of vehicles, while others are based on experiences and observations. Centralized experience-based trust models generally comprise three parts, transport authority (TA), RSUs and vehicle nodes. TA computes the trust stages of all nodes in VANETs. Every node moving on the road will check its neighbor node's behavior and report its remarks to the TA. The TA periodically updates the trust values of vehicles as reported [21].

1.5.2. Data-Oriented Trust Models (DOTM)

Unlike the entities-based models, it depends on the message itself rather than the sender's message. Piggybacking is a traditional model based on data-oriented trust models [22]. A vehicle generates and publishes a message of events in VANETS. Many vehicles receive the messages, and then most of the recipients pass them on under some rules. Every forwarder shall add their own opinion to a message formed based on their assessment and previous opinions committed by earlier forwarders. The real development of this technique is that altered nodes' opinions have different weights. A node location is nearer to the occurrence will have higher weights.

1.5.3. Combined Trust Model (CTM)

The main objects in this category are entities and data. The combined trust models estimate the nodes' trust level and calculate data trustworthiness [23].

The rest of the paper is organized as follows: Related work is explained in Section 2, while Section 3 is about phantom node selection. Results and discussions are elaborated in Section 4, while the paper is concluded with future work in Section 5.

2. Related Work

In literature, many approaches have been proposed to cope with the source location privacy in VANETs considering different parameters. Few of the relevant approaches are discussed here. In ref. [24], authors have proposed a smart energy-based source location privacy preservation approach for intersections in urban cities. Parameters such as speed, acceleration, distance, and trust were considered by applying a multi-criteria decision tool to achieve location privacy. However, essential parameters such as trust models, V2P, RSU, and TA were missing, which could have improved location preservation results. In ref. [25], the concept of dynamic pseudonym has been used instead of vehicle ID to disguise adversary. A dynamic grouping and virtual pseudonym-changing method are proposed in which, based on status, dynamic groups are created with changing pseudonyms. High-level petri nets are used for modeling the proposed scheme. The authors claim the lowering of location traceability, minimizing computation cost, and enhanced anonymity. However, the proposed scheme is limited to low-traffic areas such as highways.

In ref. [26], a conditional privacy scheme using a pseudonym mechanism is proposed, which utilizes the technique of full aggregation to reduce bandwidth resources and computation overhead. The collected pseudo-identities are used only once to target Type-I and Type-II adversaries in the random oracle under the computational Diffie-Hellman assumption. The authenticity of messages must be guaranteed to ensure driver personal information is not disclosed and identify actual identity in case of emergency or accident. The authors in [27] proposed a robust scheme that works on conditional privacy preservation with mutual authentication. The area roads are geographically distributed in several domains, where each domain stores certificate revocation lists in roadside units. The scheme revolves around elliptic curve cryptography using a one-way hash function excluding complex operations. The scheme reduces computation cost by 13.3% while reducing communication costs in signing and verifying messages up to 99.85% and 99.93%. However, some of the limitations of the presented approach are frequent tradeoffs, dependencies on RSU, and complexity [26,27].

The authors in [28] used a statistical method and a traffic model to identify false information attacks, particularly on emergency messages and malicious vehicles. The IDS is implemented at each node and can identify and control the disruption by corrective action using the statistical method. Parameters such as speed, an average of calculated flow, and an average of density were considered to exchange information using the Green Shields model. The mean value of each vehicle is calculated and compared with every other node. Every node in the particular location will compute the exact flow value. The *t*-test is then used to detect any malevolent node reporting a false value. This method does not recognize the malevolent vehicle when the malevolent vehicle coordinates and varies

the value of the parameter to match the flow value received with computed values. The overhead of the proposed IDS increases as several malevolent vehicles increase.

A P^4QS peer-to-peer privacy security query service structure was suggested in [29], which enables anonymous agents to produce false locations to replace cooperative vehicle locations. However, it does not consider the issue of common trustworthiness among nodes. The authors in [30] presented a reputation system calculated by nodes to identify the malevolent vehicles. However, the process of malevolent assessment needs improvement as it cannot afford the actual joint trust among the nodes. Moreover, the created anonymous hiding areas cannot efficiently secure the privacy of nodes.

In ref. [31], the authors proposed a trust model (LSOT) in VANETs based on certificate and recommendation. The LSOT model works in a distributed manner. To compute the trust model, three kinds of weight features are used: numbers, time decay, and context to correctly control the complete trust. The model's main limitation is distinguishing among the messages and trust of the vehicles.

A trust model DMN in VANETs based on a cluster-based mechanism has been proposed by Khan et al. in [32]. It is the responsibility of the cluster head (CH) to compute the trust and forward it to a trusted authority. In addition, based on data obtained from CH, the trusted authority is responsible for removing a malicious node from the network. Due to continuous reporting, this approach is highly over-generated, reducing network performance. In addition, the information of network contact between CH, TA, and nodes is incomplete. A trust model framework based on selection of CH and reputation was proposed by Jesudoss et al. in [33]. The truth-telling method was adopted to achieve a better reputation. Moreover, in the selection, by using weights, nodes grant incentives. The greater the weight, the higher the node is trusted by CH. One of the limitations of this approach is that it suffers from a rural and highly moveable scenario where few vehicles are involved in the selection.

Zhang et al. discussed a trust mechanism built on the Chinese remainder theorem (CRT) [34]. Authors provide authentication focused on protecting the privacy of nodes. The mechanism is grounded on tamper-proof device (TPD) identification, RSU, and TA. The limitation of the suggested technique is that it is entirely centralized, relies on RSU and TA, which makes it impracticable in rural areas. In ref. [35], the authors proposed a trust system created on fuzzy logic that directly calculates trust on the vehicles. The authors used honesty, cooperativeness, and responsibility as parameters for calculating trust. The key drawback is the coverage area limitation due to the decentralization approach.

A hybrid dual-mode trust management scheme for vehicular networks was proposed by Rai et al. [36]. The proposed scheme applies to both phenomena of urban and rural. The system is based on a credit method, in which the value is calculated by using the history of the sender and validation of the received message. The main drawback is the absence of V2I and central authority.

In this study, we used to trust in both phenomena of VANETs. Firstly, the source propagates a beacon message to accumulate trust values in the radio range to select the phantom node and remove malicious nodes in the communication range. Secondly, source nodes will calculate the local degree of trust among V2V as Criteria 1 and 3 to select phantom nodes in the absence of an infrastructure network. On the other hand, if the infrastructure is available, then the source vehicle calculates the degree of trust globally with the help of all criteria through RSU to select the phantom node and pinpoint the malicious node on a certain threshold. If a node trust value is below the threshold, it will mark as a malevolent node and will not participate in the communication. If the malicious node is found un-cooperated, the RSU will blacklist it and transmit the identification and trust values of malicious node to the neighbor RSUs to block the particular node for additional communication. Moreover, the particular node will not communicate elsewhere with neighbors within a network.

The innovation of the PTR model includes a trust-based phantom node selection that is proficient through different parameters, e.g., reputation, knowledge, history, and

experience-based. A vigorous credentials of a malevolent node with the advantage of trust criteria. Moreover, the PTR model presents the trust transmission and accumulation technique that permits RSUs to share the level of trust of the specific node. Furthermore, it is responsible and capable of collecting earlier trust levels with the updated level of trust. In this model, we have used numerous distinctive trust parameters such as entity-oriented, data-oriented, and combined trust models to design the PTR model having the capability to cope with various attacks and hide the source location privacy.

3. Phantom Node Selection

In the proposed model, selecting multiple phantom nodes while considering multiple criteria makes it a multi-criteria decision-making (MCDM) problem. The MCDM has several complex applications for decision-making. As previously mentioned, the selection of a phantom node uses a multi-criteria decision tool (i.e., ANP). The analytic network process (ANP) now captures various aspects of silent expertise. Elements are diagrammed into clusters of related factors, and links are made to several elements from a parent factor in a cluster, such as the decision-making alternatives in another cluster, as illustrated in Figure 2. They can influence the parent, or the parent can influence them by comparison to define their priorities. In literature, different clustering mechanisms are used to categorize nodes into different clusters [37,38]. There are clusters, elements, and connections within a network. A simple network may be expanded to include dynamic, multistage network models of advantages, incentives, costs, and risks.

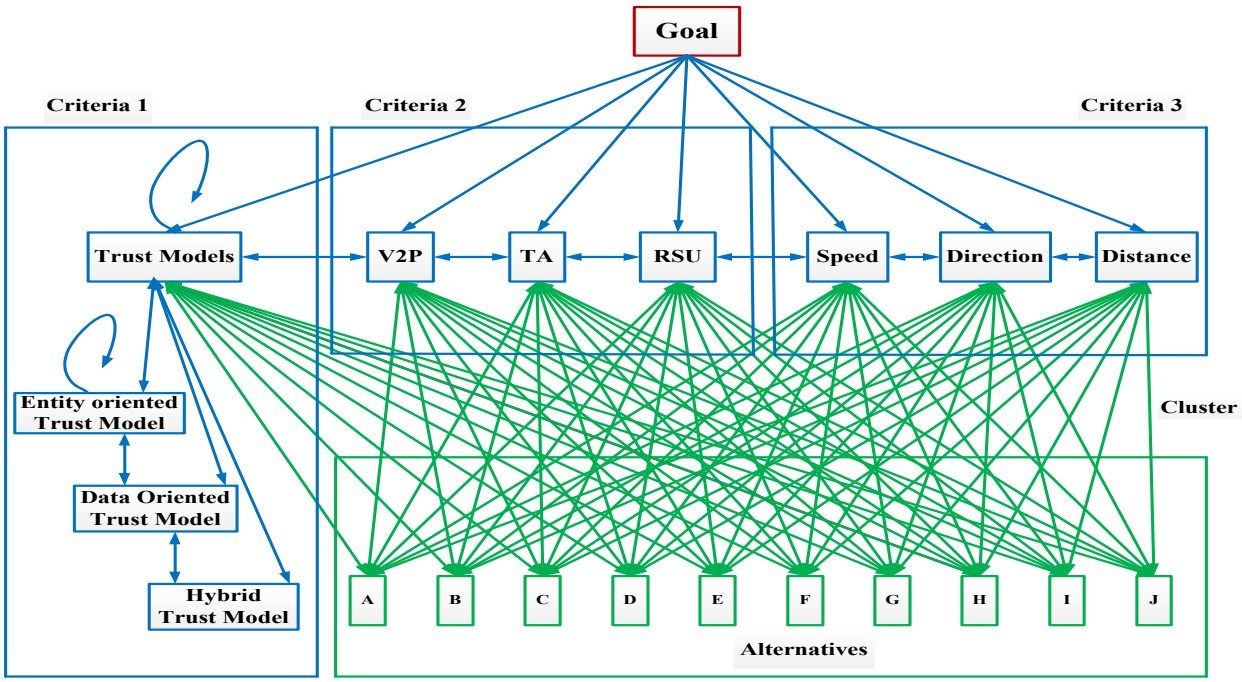

Figure 2. Pairwise comparison.

The ANP technique is used to measure the weighing importance of every factor in decision-making. ANP applies dynamic hierarchical, network dependence, and multiple indices to decision-making issues. The relativity or weight of alternatives is determined by each criterion involved in a particular decision-making problem. In general, four steps are taken in determining the weight of the decision-making factor at the network level: first, we create a network model, second is building judgment matrices, then third is to checking the consistency and ranking, and lastly, a synthesis and consistency check.

3.1. System Model

Traffic moves on a double road in both directions in the proposed scenario. The vehicular network model comprises three criteria (Criteria 1, Criteria 2, and Criteria 3), each criterion having three parameters, as shown in Figure 2. Criteria 1 includes an entity-oriented trusted model, data-oriented trust model, and combined trust model, Criteria 2 has TA, RSUs, and vehicle-to-pedestrian (V2P), and distance, direction, and speed are in Criteria 3.

- In V2V communication (if there is no infrastructure), the source vehicle wants to share information messages, first of all, and source nodes scan the communication range. During the scanning, the source node receives alternative values of the trust model from Criteria 1, 2, and 3, as shown in Figure 3, a and c. ANP is applied to rank and select trustworthy phantom nodes on the basis of criteria above.
- V2I communication is the wireless exchange of data among vehicles and roadside. In the presence of the V2I scenario, the source node will scan the radio range along with infrastructure and accumulate the trust values of nodes and the infrastructure network, as shown in Figure 3b. The source node may obtain the trust level from the network. The decision of phantom selection is based on Criteria 1, 2, and 3.

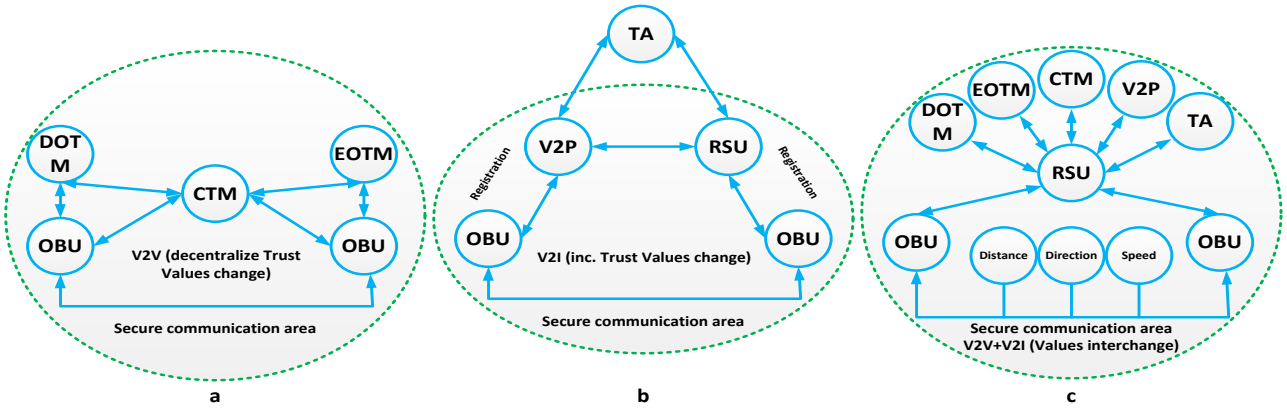

Figure 3. System model. (**a**) Criteria 1 (**b**) Criteria 2 (**c**) Criteria 3.

The proposed privacy preserved trust relationship model (PTR) is lightweight, having a smaller number of arithmetic processes thatused to decrease the complexity of the model, e.g., eigen values, eigen vectors, and multipart mathematics. Trustworthiness consists of numerous phases to compute trust received from the sender. In PTR, the model is a hybrid that computes trust in content and context-based on V2V and V2I communications. The PTR model includes the trust estimation and decision model.

3.1.1. Trust Estimation Model

The trust estimation is achieved considering all parameters defined in all three criteria to compute trust values. The vehicles share information from neighbor vehicles or the infrastructure network.

3.1.2. Decision Model Process

In the proposed PTR model, the trust values from nodes in the communication range are based on a threshold value to decide whether to process the message or discard it. If the node's trust value is less than the threshold, the phantom node rejects the node and marks it as a malicious node and then updates the database. If the value exceeds the threshold, it means it is a normal node and ranked (phantom node) based on the respective trust value.

This study proposed the following method for protecting the source location privacy of a vehicle. Firstly, the PTR model values of parameters are graded and compared. Based on this, we have calculated the alternatives (nodes) grading and compared it with all criteria based on the number of requests made and positive responses in communication

scenarios (e.g., highway, traffic red-light, traffic congestion, parking, and shopping malls). In this case, the trust ratio of the data is computed. Each vehicle gives a positive response to the information, which will be given a reward score by providing true information to calculate the credibility of each node in a network.

In the second case, if the infrastructure is available, the source node will use RSU, TA, and V2P to confirm the trustworthiness values of each node in a network and take the responsibility to select the trustworthy node as a phantom node. Figure 4 illustrates the proposed PTR model's complete description and process flow.

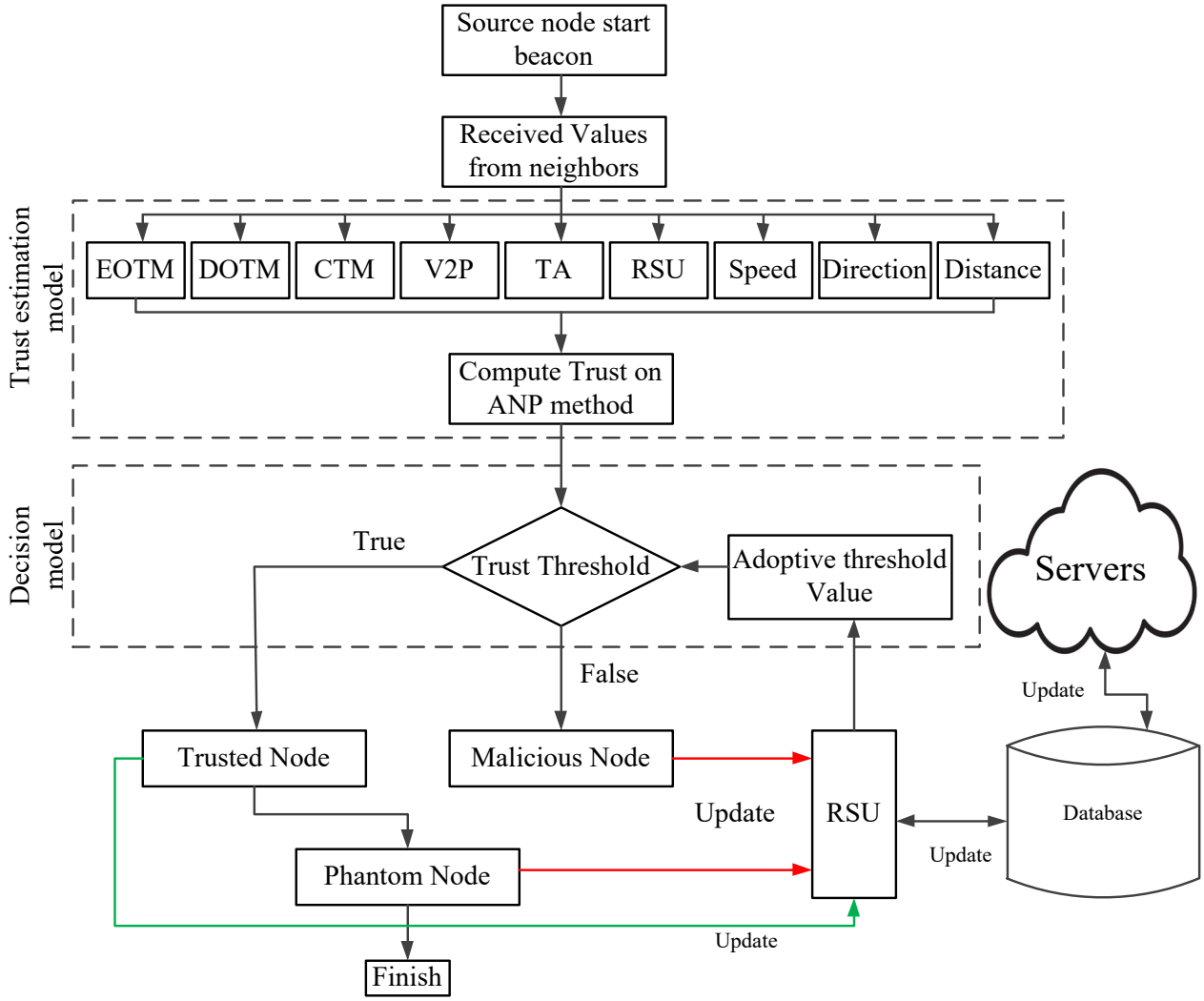

Figure 4. Proposed PTR model.

The system model is represented in Figure 5, in which different nodes are represented through different colors. It can be seen in the figure that communication can be possible through V2V, V2I, V2P, and RSU. The source node propagates a beacon message to the neighboring nodes to receive trust values. The source node applies the PTR model to compute trust values for phantom node selection. Malicious nodes will be removed (if any) based on the threshold value. Once the phantom nodes are selected, each node will communicate through them that fall within their communication range. All nodes can acquire information through phantom nodes from the neighbor nodes for safe and secure driving. RSUs are deployed at regular intervals as infrastructure entities. RSU has responsibilities such as nodes to access the network, delivering trust values for vehicles, and sending information between TA and them.

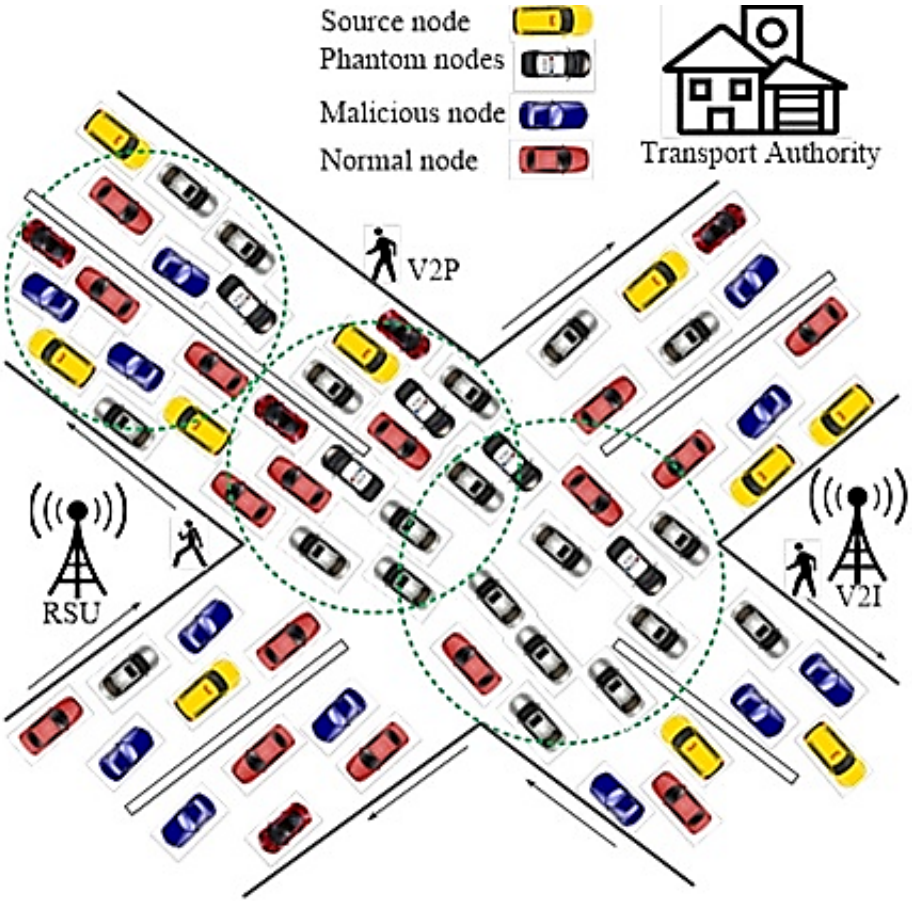

Figure 5. System Model.

The relative significance (shown in Table 2) of the individual element of a layer to the elements of the above-noted layer can be extracted after constructing the comparison matrix. In case of a comparison matrix, normalization of the eigenvector conforming to the eigenvalue of the judgment matrix can calculate the relative importance. The established matrices of judgment quantify the judgment. However, there may be inconsistencies when many parallel comparisons are conducted. The matrix consistency assessment aims to monitor the consistency of the assessment and ensure that every judgment is rational, avoiding any contradictory outcome. When the consistency rate (CR) is below 10%, the judging matrix shall be deemed to be consistent [39,40]. A consistency index (CI) can be calculated by Equation (1), where λ max is the maximum eigenvalue.

$$\mathrm{CI} = \frac{\lambda \mathrm{max} - \mathrm{n}}{\mathrm{n} - 1}, \mathrm{n} = 1, 2, \ldots, 9 \tag{1}$$

Then, the CR is acquired by dividing CI by the random consistency index (RI) as shown in Equation (2), as the values of RI against each element are shown in Table 3.

$$\mathrm{CR} = \frac{\mathrm{CI}}{\mathrm{RI}} \tag{2}$$

Table 2. I The intensity of relative importance.

Strength of Relation	Description
1	Equal significance
3	Reasonable significance
5	Robust significance
7	Established significance
9	Complete significance
2, 4, 6, 8	In-between score between two neighboring values
Reciprocal Values	The judgment score of the importance of the element i and j is R_{ij}, and the reciprocal value is $1/R_{ij}$

Table 3. The RI Values.

Elements	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
RI	0	0	0.58	0.9	1.12	1.26	1.36	1.41	1.45	1.49	1.51	1.53	1.56	1.57	1.59

3.2. Limit Matrix

The Limit (resultant) matrix is acquired from the weighted matrix to attain stable values. It contains a summary of all pairwise comparisons made having an indirect relationship among elements. Table 4 shows the weights of alternatives and criteria. It can be seen in Table 4 that node G has the maximum weight and hence selected as a phantom node, followed by node I as the second highest weight. For instance, nodes B and J have the minimum weights. Therefore, both are selected as malicious nodes based on threshold, as shown in Table 4. Moreover, the limit matrix can be beneficial in ranking the criteria as it contains the weights of criteria as well.

Table 4. Limit matrix.

		Alternatives										Criteria 1			Criteria 2			Criteria 3		
		A	B	C	D	E	F	G	H	I	J	CT	DOT	EOT	RSU	TA	V2P	DR	Distance	Speed
Alternatives	A	0.020	0.020	0.020	0.020	0.020	0.020	0.020	0.020	0.020	0.020	0.020	0.020	0.020	0.020	0.020	0.020	0.020	0.020	0.020
	B	0.011	0.011	0.011	0.011	0.011	0.011	0.011	0.011	0.011	0.011	0.011	0.011	0.011	0.011	0.011	0.011	0.011	0.011	0.011
	C	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019
	D	0.022	0.022	0.022	0.022	0.022	0.022	0.022	0.022	0.022	0.022	0.022	0.022	0.022	0.022	0.022	0.022	0.022	0.022	0.022
	E	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019
	F	0.021	0.021	0.021	0.021	0.021	0.021	0.021	0.021	0.021	0.021	0.021	0.021	0.021	0.021	0.021	0.021	0.021	0.021	0.021
	G	0.029	0.029	0.029	0.029	0.029	0.029	0.029	0.029	0.029	0.029	0.029	0.029	0.029	0.029	0.029	0.029	0.029	0.029	0.029
	H	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019	0.019
	I	0.024	0.024	0.024	0.024	0.024	0.024	0.024	0.024	0.024	0.024	0.024	0.024	0.024	0.024	0.024	0.024	0.024	0.024	0.024
	J	0.012	0.012	0.012	0.012	0.012	0.012	0.012	0.012	0.012	0.012	0.012	0.012	0.012	0.012	0.012	0.012	0.012	0.012	0.012
Criteria 1	CT	0.115	0.115	0.115	0.115	0.115	0.115	0.115	0.115	0.115	0.115	0.115	0.115	0.115	0.115	0.115	0.115	0.115	0.115	0.115
	DOT	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039
	EOT	0.112	0.112	0.112	0.112	0.112	0.112	0.112	0.112	0.112	0.112	0.112	0.112	0.112	0.112	0.112	0.112	0.112	0.112	0.112
Criteria 2	RSU	0.096	0.096	0.096	0.096	0.096	0.096	0.096	0.096	0.096	0.096	0.096	0.096	0.096	0.096	0.096	0.096	0.096	0.096	0.096
	TA	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045
	V2P	0.124	0.124	0.124	0.124	0.124	0.124	0.124	0.124	0.124	0.124	0.124	0.124	0.124	0.124	0.124	0.124	0.124	0.124	0.124
Criteria 3	DR	0.141	0.141	0.141	0.141	0.141	0.141	0.141	0.141	0.141	0.141	0.141	0.141	0.141	0.141	0.141	0.141	0.141	0.141	0.141
	Distance	0.059	0.059	0.059	0.059	0.059	0.059	0.059	0.059	0.059	0.059	0.059	0.059	0.059	0.059	0.059	0.059	0.059	0.059	0.059
	Speed	0.065	0.065	0.065	0.065	0.065	0.065	0.065	0.065	0.065	0.065	0.065	0.065	0.065	0.065	0.065	0.065	0.065	0.065	0.065

4. Results and Discussion

To obtain the ranking of all alternatives and criteria in a given scenario for decision-making, the ANP method is repeated to compare all elements to get a limit matrix. The result illustrates that node *G* has the maximum weight (i.e., 0.147), thus selected as a phantom node, and the second candidate is node I having 0.122 value as shown in Figure 6.

The result indicates that Nodes B and J have minimum weights, i.e., 0.056 and 0.063, respectively, thus marked as malicious nodes as shown in Figure 6.

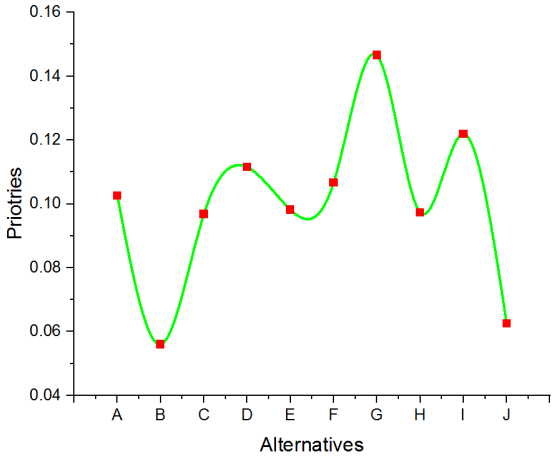

Figure 6. Comparison of Alternatives.

4.1. Sensitivity Analysis

Sensitivity analysis is greatly endorsed to analyze the stability of the elements. It is used to examine the outcomes and position of elements (alternatives) gained using ANP model. In a weighted matrix, it is to be measured that all alternative's elements are subjective by the elements in criteria (parameters). To begin the sensitivity analysis, the first highest weight element is identified. A sensitivity analysis can also deliver decision-making perceptions to the result of a particular scenario. If a priority of criteria is reformed, then it will change the ranking of the alternatives as well. The sensitivity analysis is performed by exchanging every parameter's weight with another parameter by keeping the weights of other criteria constant [41]. Criteria 3 is selected to check the sensitivity of parameters (distance and speed) assign weights to parameters (e.g., lowest, average and highest). The complete process of ANP is applied to the entire network to gain the new final priorities of alternatives (nodes). The results are shown in Figure 7 that shows the impact of distance parameter on alternatives and changed their weights. Node G is in high rank with weight 0.14652, 0.14656 and 0.1466, respectively. Node B has the lowest ranking weights 0.05773, 0.05685, and 0.05598 according to (lowest, average and highest) weights as shown in Figure 7a.

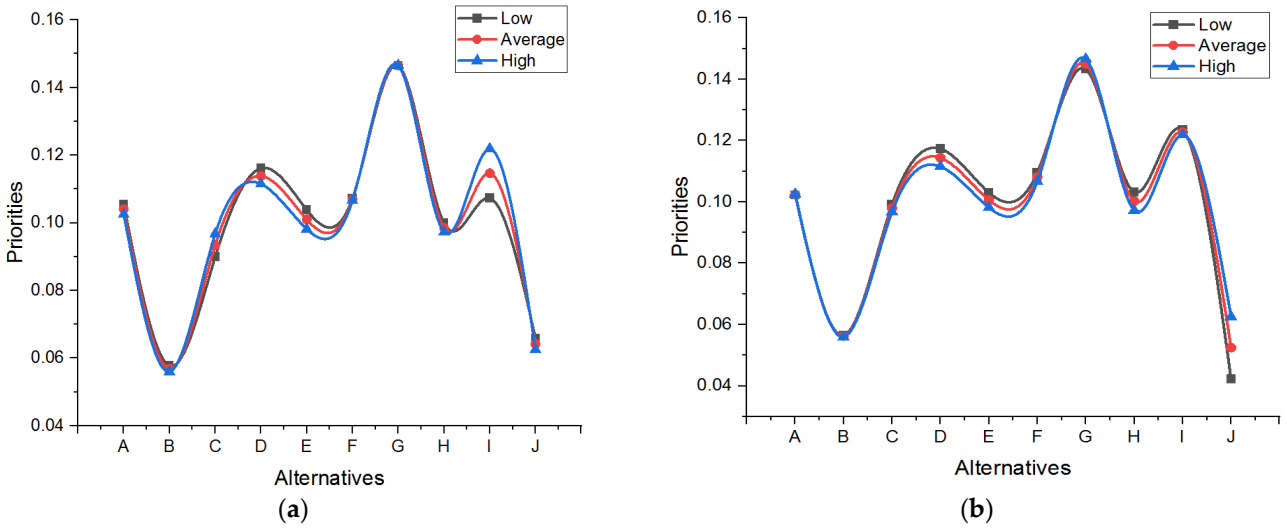

Figure 7. Distance and Speed Variance in Criteria 3. (**a**) Variation in Distance (**b**) Variation in Speed.

Speed parameter variation also affects the alternatives weights. After performing these variations, Node G still has high weights (0.14321, 0.14492, and 0.1466), whereas Nodes B and J have low priority in all aspects, as shown in Figure 7b.

4.2. Influence of Criteria

Figure 8 shows the impact of Criteria 1 (CTM, DOTM and EOTM) on alternatives. The graph shows that each parameter has an influence on each node. The parameters influence on Node G is (i.e., 0.147, 0.157) respectively, thus selected as a phantom node(a), Node I has second maximum values (0.128,0.123 and 0.128) and selected as phantom node (b), Node D has third number as maximum values of (0.125,0.114 and 0.122) as shown in Figure 8. The result shows that Node B has the minimum weight (i.e., 0.051, 0.057 and 0.054), thus remarked as a malicious node, Node J is below the threshold value so marked as malicious node as well.

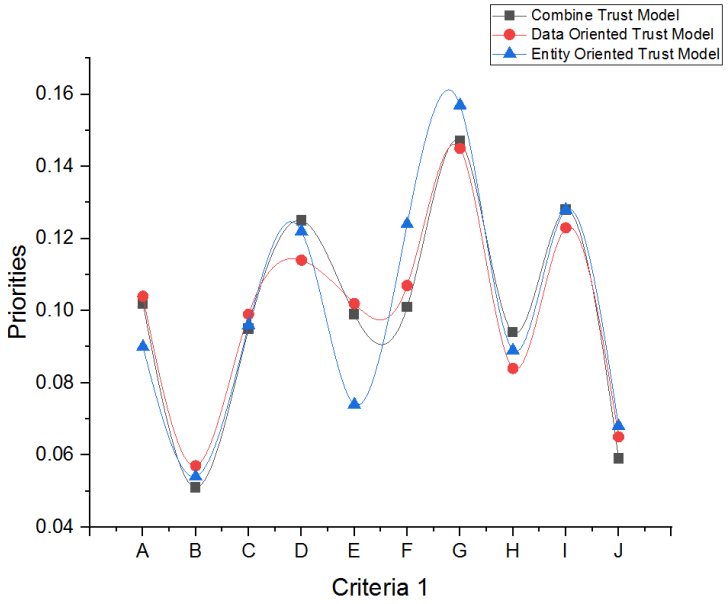

Figure 8. The Criteria 1 Influence on Alternatives.

The impact of Criteria 2 (RSU, TA, and V2P) on alternatives is shown in Figure 9.

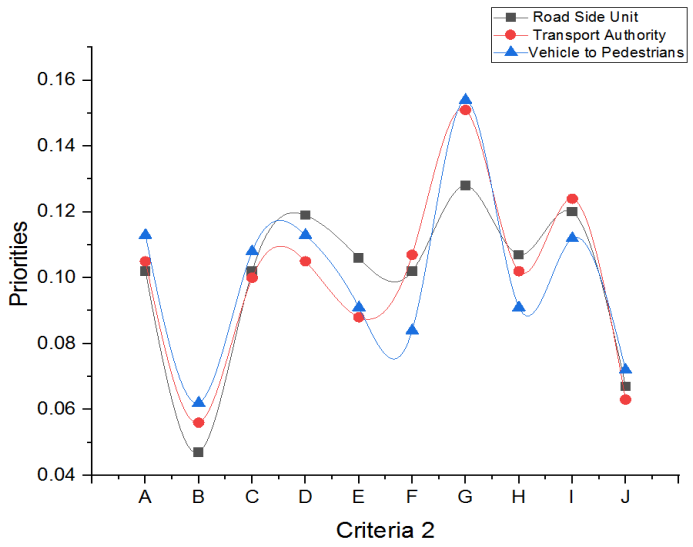

Figure 9. Criteria 2 Influence on Alternatives.

It concludes that Node (G) has the highest priority thus selected as a phantom node on all aspects of criteria. In contrast, Nodes (B) and (J) are marked as malicious due to minimum priority weights as shown in Figures 8 and 9, respectively.

5. Conclusions and Future Work

Numerous privacy preservation methods for VANETs have been proposed, but every method has its own limitations. Most of the current approaches focus only on content privacy development by avoiding context privacy aspects. Moreover, the current privacy preservation models use a single trust parameter such as history-based trust, indirect or direct trust model, acceleration, Euclidean distance, etc., to choose a cluster head node. These parameters may allow selecting a cluster head node nonetheless do not provide a safe way to frame trustworthy communication. Most of the existing source location privacy techniques do not report this problem and lack in conveying trustworthy communication. In this paper, a privacy-preserving trust relationship (PTR) model is proposed to address these context privacy problems. PTR offers a method to formulate trustworthiness and secure communication.

Moreover, a node with optimal trust value and all parameters is elected as a phantom node based on threshold values, which enhances trusted communication among nodes to believe in information produced by a vehicle. The PTR model scans the network and marks the malicious node based on threshold. Furthermore, the proposed work is improved by using different trust parameters to come up with the most optimal phantom node to preserve the location privacy of a vehicle. Sensitivity analysis is performed to check the impact of one parameter over other to come up with the most significant parameter.

In the future, we are aiming to implement the proposed model in a real-time vehicle's network considering urban areas, especially at junctions in crowded regions.

Author Contributions: Conceptualization, H.F.; Formal analysis, H.F., A.K.; Supervision, N.A., M.I.; Validation, W.A., N.A.; Writing—original draft, H.F., A.K., M.A.K.; Writing—review & editing, W.A., N.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The authors wish to acknowledge the support of Prince Sultan University for paying article processing charges (APC) of this publication. The authors would like to thank Prince Sultan University for their support.

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

References

1. Toh, C.K. *Ad hoc Mobile Wireless Networks: Protocols and Systems*; Pearson Education: Upper Saddle River, NJ, USA, 2001.
2. Rehman, O.; Ould-Khaoua, M. A hybrid relay node selection scheme for message dissemination in VANETs. *Future Gener. Comput. Syst.* **2019**, *93*, 1–17. [CrossRef]
3. Wan, J.; Liu, J.; Shao, Z.; Vasilakos, A.V.; Imran, M.; Zhou, K. Mobile crowd sensing for traffic prediction in internet of vehicles. *Sensors* **2016**, *16*, 88. [CrossRef] [PubMed]
4. Sommer, C.; Dressler, F. *Vehicular Networking*; Cambridge University Press: Cambridge, UK, 2015.
5. Jan, B.; Farman, H.; Khan, M.; Talha, M.; Din, I.U. Designing a smart transportation system: An Internet of things and big data approach. *IEEE Wirel. Commun.* **2019**, *26*, 73–79. [CrossRef]
6. Farman, H.; Javed, H.; Jan, B.; Ahmad, J.; Ali, S.; Khalil, F.N.; Khan, M. Analytical network process based optimum cluster head selection in wireless sensor network. *PLoS ONE* **2017**, *12*, e0180848. [CrossRef]
7. Farman, H.; Jan, B.; Talha, M.; Zar, A.; Javed, H.; Khan, M.; Din, A.U.; Han, K. Multicriteria-based location privacy preservation in vehicular ad hoc networks. *Complexity* **2018**, *2018*, 1–12. [CrossRef]
8. Ali, J.; Roh, B.-h. Quality of service improvement with optimal software-defined networking controller and control plane clustering. *Comput. Mater. Contin.* **2021**, *67*, 849–875. [CrossRef]
9. Latif, S.; Mahfooz, S.; Jan, B.; Ahmad, N.; Farman, H.; Khan, M.; Javed, H. Multicriteria based next forwarder selection for data dissemination in vehicular ad hoc networks using analytical network process. *Math. Probl. Eng.* **2017**, *2017*, 1–18. [CrossRef]
10. Parent, W.A. Privacy, morality, and the law. *Philos. Public Aff.* **1983**, *12*, 269–288.
11. Ling, J.; Xu, J. Decentralized Location Privacy Protection Method of Offset Grid. In Proceedings of the 3rd International Conference on Mechatronics Engineering and Information Technology (ICMEIT 2019), Dalian, China, 29–30 March 2019.

12. Zhu, L.; Gai, K.; Li, M. Security and Privacy Issues in Internet of things. In *Blockchain Technology in Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 29–40.
13. Jøsang, A.; Golbeck, J. Challenges for robust trust and reputation systems. In Proceedings of the 5th International Workshop on Security and Trust Management (SMT 2009), Saint Malo, France, 24–25 September 2009; p. 52.
14. Raya, M.; Papadimitratos, P.; Gligor, V.D.; Hubaux, J.-P. On data-centric trust establishment in ephemeral ad hoc networks. In Proceedings of the IEEE INFOCOM 2008—The 27th Conference on Computer Communications, Hangzhou, China, 30 July–2 August 2018; pp. 1238–1246.
15. Dotzer, F.; Fischer, L.; Magiera, P. Vars: A vehicle ad-hoc network reputation system. In Proceedings of the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, Taormina, Italy, 13–16 June 2005; pp. 454–456.
16. Golle, P.; Greene, D.; Staddon, J. Detecting and correcting malicious data in VANETs. In Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, Philadelphia, PA, USA, 1 October 2014; pp. 29–37.
17. Minhas, U.F.; Zhang, J.; Tran, T.; Cohen, R. Towards expanded trust management for agents in vehicular ad-hoc networks. *Int. J. Comput. Intell. Theory Pract.* **2010**, *5*, 3–15.
18. Chen, C. *A Trust-Based Message Evaluation and Propagation Framework in Vehicular Ad-Hoc Networks*; University of Waterloo: Waterloo, ON, Canada, 2010.
19. Gerlach, M. Trust for vehicular applications. In Proceedings of the Eighth International Symposium on Autonomous Decentralized Systems (ISADS'07), Sedona, AZ, USA, 21–23 March 2007; pp. 295–304.
20. Patwardhan, A.; Joshi, A.; Finin, T.; Yesha, Y. A data intensive reputation management scheme for vehicular ad hoc networks. In Proceedings of the 2006 3rd Annual International Conference on Mobile and Ubiquitous Systems-Workshops, San Jose, CA, USA, 17–21 July 2006; pp. 1–8.
21. Li, Q.; Malip, A.; Martin, K.M.; Ng, S.-L.; Zhang, J. A reputation-based announcement scheme for VANETs. *IEEE Trans. Veh. Technol.* **2012**, *61*, 4095–4108.
22. Huang, Z.; Ruj, S.; Cavenaghi, M.A.; Stojmenovic, M.; Nayak, A. A social network approach to trust management in VANETs. *Peer-to-Peer Netw. Appl.* **2014**, *7*, 229–242. [CrossRef]
23. Monir, M.; Abdel-Hamid, A.; El Aziz, M.A. A categorized trust-based message reporting scheme for VANETs. In Proceedings of the International Conference on Security of Information and Communication Networks, Canterbury, UK, 6–9 September 2021; pp. 65–83.
24. Farman, H.; Jan, B.; Khan, Z.; Koubaa, A. A smart energy-based source location privacy preservation model for Internet of things-based vehicular ad hoc networks. *Trans. Emerg. Telecommun. Technol.* **2020**, 1–14. [CrossRef]
25. Ullah, I.; Shah, M.A.; Khan, A.; Maple, C.; Waheed, A. Virtual Pseudonym-Changing and Dynamic Grouping Policy for Privacy Preservation in VANETs. *Sensors* **2021**, *21*, 3077. [CrossRef]
26. Mei, Q.; Xiong, H.; Chen, J.; Yang, M.; Kumari, S.; Khan, M.K. Efficient certificateless aggregate signature with conditional privacy preservation in IoV. *IEEE Syst. J.* **2020**, *15*, 245–256. [CrossRef]
27. Al-Shareeda, M.A.; Anbar, M.; Hasbullah, I.H.; Manickam, S.; Hanshi, S.M. Efficient conditional privacy preservation with mutual authentication in vehicular ad hoc networks. *IEEE Access* **2020**, *8*, 144957–144968. [CrossRef]
28. Zaidi, K.; Milojevic, M.B.; Rakocevic, V.; Nallanathan, A.; Rajarajan, M. Host-based intrusion detection for vanets: A statistical approach to rogue node detection. *IEEE Trans. Veh. Technol.* **2015**, *65*, 6703–6714. [CrossRef]
29. Ghaffari, M.; Ghadiri, N.; Manshaei, M.H.; Lahijani, M.S. P^4QS: A peer-to-peer privacy preserving query service for location-based mobile applications. *IEEE Trans. Veh. Technol.* **2017**, *66*, 9458–9469. [CrossRef]
30. Luo, B.; Li, X.; Weng, J.; Guo, J.; Ma, J. Blockchain enabled trust-based location privacy protection scheme in VANET. *IEEE Trans. Veh. Technol.* **2019**, *69*, 2034–2048. [CrossRef]
31. Liu, Z.; Ma, J.; Jiang, Z.; Zhu, H.; Miao, Y. LSOT: A lightweight self-organized trust model in VANETs. *Mob. Inf. Syst.* **2016**, *2016*, 7628231. [CrossRef]
32. Khan, U.; Agrawal, S.; Silakari, S. Detection of malicious nodes (DMN) in vehicular ad-hoc networks. *Procedia Comput. Sci.* **2015**, *46*, 965–972. [CrossRef]
33. Jesudoss, A.; Raja, S.K.; Sulaiman, A. Stimulating truth-telling and cooperation among nodes in VANETs through payment and punishment scheme. *Ad Hoc Netw.* **2015**, *24*, 250–263. [CrossRef]
34. Zhang, J.; Cui, J.; Zhong, H.; Chen, Z.; Liu, L. PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 722–735. [CrossRef]
35. Guleng, S.; Wu, C.; Chen, X.; Wang, X.; Yoshinaga, T.; Ji, Y. Decentralized trust evaluation in vehicular Internet of things. *IEEE Access* **2019**, *7*, 15980–15988. [CrossRef]
36. Rai, I.A.; Shaikh, R.A.; Hassan, S.R. A hybrid dual-mode trust management scheme for vehicular networks. *Int. J. Distrib. Sens. Netw.* **2020**, *16*, 1550147720939372. [CrossRef]
37. Tsiropoulou, E.E.; Paruchuri, S.T.; Baras, J.S. Interest, energy and physical-aware coalition formation and resource allocation in smart IoT applications. In Proceedings of the 2017 51st Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, USA, 22–24 March 2017; pp. 1–6.
38. Farman, H.; Jan, B.; Javed, H.; Ahmad, N.; Iqbal, J.; Arshad, M.; Ali, S. Multi-criteria based zone head selection in Internet of things based wireless sensor networks. *Future Gener. Comput. Syst.* **2018**, *87*, 364–371. [CrossRef]
39. Saaty, T.L. Decision making with the analytic hierarchy process. *Int. J. Serv. Sci.* **2008**, *1*, 83–98. [CrossRef]

40. Bhushan, N.; Rai, K. *Strategic Decision Making: Applying the Analytic Hierarchy Process*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2007.
41. Önüt, S.; Kara, S.S.; Işik, E. Long term supplier selection using a combined fuzzy MCDM approach: A case study for a telecommunication company. *Expert Syst. Appl.* **2009**, *36*, 3887–3895. [CrossRef]