Journal of
Sensor and Actuator Networks

MDPI

Article

Bring Your Own Reputation: A Feasible Trust System for Vehicular Ad Hoc Networks

Ricardo Mühlbauer and João Henrique Kleinschmidt *

Centro de Engenharia, Modelagem e Ciências Socias Aplicadas, Universidade Federal do ABC, Av. dos Estados 5001, Santo André, SP 09210-580, Brazil; ricardo.muhlbauer@ufabc.edu.br
* Correspondence: joao.kleinschmidt@ufabc.edu.br

Received: 21 July 2018; Accepted: 23 August 2018; Published: 1 September 2018

Abstract: The establishment of trust in vehicular ad hoc networks (VANETs) will require the application of non-conventional measures of information security, such as reputation of the participants. The system proposed in this paper uses the concept of certified reputation, in which vehicles communicate providing digital certificates that include their own reputation level. The vehicles periodically come in contact with certification and traffic control authorities to update their reputation levels, which are determined by the validation of their behavior on the network. Decision-making mechanisms in the receiver vehicles are responsible for evaluating whether the messages are true or false, based on the reputation of the communication nodes. The quantitative analysis of simulated scenarios showed the combination of the central reputation scheme with an appropriate vehicular decision mechanism achieved a total of correct decisions superior than without reputation systems. Considering the constraints of a high mobile network, the proposed system is a feasible way to reduce the risk of anomalous or malicious behavior in a vehicular network.

Keywords: VANETs; vehicular ad hoc networks; intelligent transportation systems; trust; reputation

1. Introduction

One of the primary goals of the interconnection of vehicles in networks is to improve road safety. However, malicious attacks or anomalous operation of communication nodes (vehicles or static units) can cause fatal accidents [1]. The loss of confidence in the system can generate rejection and derail the deployment of these networks. To enable road safety applications, periodic transmission of beacons contains accurate data of its location, which can be received by any vehicle or device in the transmission range. Developing standards recognize the importance of maintaining the privacy of the vehicle owners against possible traceability in the network. Research on vehicular ad hoc networks (VANETs) points out to the use of pseudonyms to preserve the privacy of drivers while maintaining the possibility of identification and conditioned accountability.

There are many traditional solutions for information security for the establishment of trust in VANETs [2], such as authentication, encryption, and access control, collectively known as hard security. These measures are essential to ensure the authenticity of participants in VANETs. However, these networks are characterized by the dynamism of their topology due to the high mobility of vehicles, which hinders the implementation of protection systems. As the communication often occurs between unknown nodes, the use of traditional mechanisms of information security is not enough to ensure the reliability of the network [3]. They are not effective against false messages of legitimate nodes.

To compose the trust system, we have to adopt additional mechanisms of information security described by the term soft security [2], which requires the collaboration and adherence to standards and rules for participating in a community or network. Reputation systems can be applied as a factor to promote trust in the communication between unknown entities, as in the case of vehicular networks.

They constitute a way to encourage honest collaboration between communication nodes (vehicles) while reducing or even isolating the participation of malicious nodes and anomalous functioning.

Reputation is described in [4] as a term denoting the expected future behavior of an entity based on observations or behavioral information of the past in a context and period of time. According to Ref. [5], the main purpose of reputation systems is to reduce the opportunism and vulnerability between unknown partners so that they can take risks, build trust, and decide if they want to interact. Reputation is a time sensitive concept which can evolve positively or negatively according to the behavior of the entities. For the purposes of this research, the negative evolution of the reputation of an entity is called "decay of reputation". The positive evolution of the reputation constituting its recovery after decay is called "redemption of reputation".

Most systems proposed in the literature use decentralized trust schemes, such as [4,6,7], without the need for a central system to determine the reputation of the nodes. These systems require significant processing on the nodes and communication to support behavioral validation mechanisms in the network. They also often have problems in handling the identity of the vehicle and maintenance of privacy of the drivers, causing a misalignment with the standardization under development and the field test projects of VANETs [8]. A few proposals in the literature use centralized trust schemes such as [9–11], but they rely on the frequent availability of infrastructure units, which cannot be guaranteed.

This paper proposes a centralized system for reputation in VANETs aiming to solve the shortcomings identified in the current proposals. The calculation of the reputation is centralized, but it does not interfere with the hybrid characteristic of VANETs and with the intermittent operation in an ad hoc manner. We use the concept of certified reputation and mechanisms that can coexist on the concepts and standards currently under development for VANETs, which is different from previous works. The main contribution of this paper is a framework that calculates the reputation in a centralized manner using certified reputation carried by vehicles. The system does not need a permanent connection with infrastructure in the roads and may use different methods for reputation calculation and vehicular decision mechanisms. We clearly show that the proposed system is robust to common attacks such as Sybil, Newcomer, Betrayal, and Inconsistency. The paper is structured as follows: related works are presented in Section 2, the system proposal in Section 3, the implementation of a model in Section 4, performance analysis in Section 5, and the conclusion in Section 6.

2. Related Work

2.1. Decentralized Systems

In this section, we describe some related work using decentralized and centralized systems. Among the decentralized proposals, we can cite [4,6,7,12–20]. Huynh et al. [12] presented a new concept called certified reputation for confidence in multi-agent systems. For each transaction in the network, an agent asks to the partner to evaluate its performance, so it can store and present it in future transactions as a reference of its behavior in the past. The trustor's recommendations should be digitally signed, constituting the concept of certified reputation. Ostermaier et al. [13] compared four vehicular decision mechanisms based on voting: freshest message, majority wins, majority of freshest messages, and majority of freshest messages with threshold. The latter mechanism showed the best results in the simulations.

Ryan et al. [6] reported a decision mechanism based on the Dempster-Shafer theory. In the system, trust relationships between nodes must be established and re-established frequently, depending on changes in the network and perception of the environment. The system receives messages about an event from multiple nodes and takes into account factors related to specific reliability in events, dynamic factors of location and time, default values of reliability of the event type, the role of the node, and its security level. Dötzer [4] presented the reputation system for VANETs called VARS (Vehicle Ad-hoc network Reputation System), whose confidence opinion generator processes indirect reputation, direct reputation, and recognition of situations and events. The scheme of the proposal is

to share reputation data with other nodes, adding this information to messages in a mechanism known as "opinion piggybacking". Lo et al. [14] proposed a reputation system based on events to prevent the dissemination of false traffic alert messages. They apply a simple mechanism consisting of storing a reputation value for each occurrence of incoming traffic. Whenever a vehicle detects the event with its onboard sensors, the value is incremented. When the reputation value of the event and the confidence value are above pre-defined levels, the occurrence is considered to be true and can be disseminated to the neighboring nodes.

De Paula [15] presented a reputation system for vehicular networks tolerant to delays and disconnections that requires the unique identification of vehicles in the network. Each vehicle locally stores two lists containing members considered reliable and malicious. The events reported by other vehicles are stored and evaluated later when the actual situation is known, thereby locally altering the reputation of the nodes. Ding et al. [7] proposed an event-based protocol to collect and aggregate information using fuzzy computational model to represent the reputation values. The fuzzy inference engine considers two input parameters: the role of the node at the event (rapporteur, observer, or participant) and the timestamp (old or new) of the occurrence from the events.

Huang [16] described how simple voting systems can lead to cascading and oversampling of information about events and proposed a system to reduce the impact of these occurrences on the network. The detection mechanism of anomalous node is based on the observation of the node movement after sending warnings and messages. Marmol et al. [17] presented a proposal of a trust and reputation system based on infrastructure for vehicular networks called TRIP (Trust and Reputation Infrastructure-based Proposal). A value of reputation is calculated for each node, taking into account three sources of information: previous direct experience with the node, recommendations from other nodes in the neighborhood, and the recommendation provided by a central authority through a RSU (Road Side Units).

Jalali et al. [18] proposed a reputation system based on fuzzy logic for VANETs. The scheme does not depend on the opinions of a node about its neighbors, which are a serious problem in reputation systems. Thus, erroneous judgments are eliminated. However, the system handles basically with the selfish behavior of the nodes, making sure that they relay event information to their neighbors. Fernandes [19] proposed a decentralized system to assess the reliability of the nodes in vehicular networks. The schema uses reputation lists of the nodes, global reputation calculated by Bayesian analysis, and voting systems for decision making. The scheme requires setting a unique network identity for the vehicle. Yang [20] described a framework for managing reputation and trust based on a mining technique to identify messages or vehicles by similarity. This paper proposed an algorithm for evaluating reputation based on similarity theory.

2.2. Centralized Systems

Among the centralized proposals, we can cite [9–11]. Park et al. [9] proposed a reputation calculation scheme based on the premise that most vehicles perform the same route daily. RSU units could perform vehicle behavior observations to build long-term reputation levels for each local community vehicles. Li et al. [10] presented a reputation scheme for VANETs based on the assessments reported by the communication nodes in relation to each other. In this mechanism, the vehicles receive event messages and keep the identity of the issuer vehicle. When the vehicle detects the same event, it can attest the validity of the received message creating a reliable value for the issuer vehicle, which will be sent to a central reputation server. This, in turn, employs a reputation aggregation algorithm to calculate a level of reputation for each vehicle that will be included in digital certificates. Liao et al. [11] proposed an approach to determine the likelihood of accuracy of incident messages transmitted from vehicle to vehicle, based on the reliability of the generator of messages and vehicles that forward them. The scheme takes advantage of the communication facilities with RSU infrastructure managed by central authorities of transit. The data are combined with a decision strategy based on thresholds.

2.3. Shortcomings in Current Proposals

For reputation systems, the maintenance of behavior statistics for an entity requires some form of persistent identification [21]. Therefore, the relationship between trust and privacy is a tradeoff, where more confidence requires less privacy and vice versa. The fully decentralized reputation systems generally require a fixed identity, since the assignment of reputation levels to pseudonyms makes difficult the decentralized administration because pseudonyms need to be changed frequently.

Systems that do not have a central authority and allow nodes to create their own pseudonyms are subject to Sybil attacks [22]. The authors in [23] describe that, in the absence of an identity management infrastructure, the calculated values of global reputation for an open number of participants can always be subverted by a Sybil attack. The development of completely decentralized reputation and trust systems [24] involves complex algorithms that require high coordination costs and processing time on the network and on the participating nodes, which may make them unfeasible. Therefore, a reputation mechanism with central coordinating authority may be more practical.

In decentralized reputation systems, each participant is responsible for gathering and assessing the other participants. The aggregation of all interactions is often impossible or very costly, so that the mechanisms must operate with a subset of evaluations. The storage approach of fully distributed form of reputation information involves unresolved problems. The difficulty of reencounter of nodes and the complexity of dissemination of reputation in the network and for nodes to exchange assessments with each other require the decentralized mechanisms to collect and process a large amount of data, which demands high traffic on the control channel. The impact of the congestion on the communication channel must be considered in the implementation of information security mechanisms in VANETs. In decentralized reputation systems, each node is responsible for determining its own estimates of reliability on the other participants of the network. There is no global or public assessment of the reputation of the nodes [25]. This issue makes it difficult for a vehicle with poor reputation to redeem and recover its reputation, since the reputation is decentralized in each network node.

Unlike the centralized system in which revocation is decided by a responsible authority, in the decentralized system, the vehicles may have totally different opinions among themselves according to the data and experiences they have at their disposal, making the consensus difficult for the revocation of vehicle certificates. The disadvantages of the centralized reputation systems are the lack of RSU units (especially in the introduction phase of VANETs), the scalability of the network in relation to the capacity of the central entities, and the problem of the single point of failure.

2.4. Comparative Analysis of Schemes

Table 1 summarizes the related works and the proposed system according to the characteristics of reputation systems that deal with the topic of this article. Most of the works uses decentralized reputation administration, but issues related to identity and privacy of the participants in the network, robustness of reputation against information security attacks, and communication system overload analysis are frequently not considered in the systems.

Table 1. Qualitative comparison of works.

Author	Administration	Reputation Mechanism	Privacy	Robustness	Network Impact	Vehicular Decision
Ostermaier et al. (2007)	Decentralized	Not Addressed	Not Addressed	Not Addressed	Not Addressed	Voting
Raya et al. (2008)	Decentralized	Dempster-Shafer	Pseudonym	Not Addressed	Not Addressed	Data Centered
Dötzer (2008)	Decentralized	Summation	Fixed Pseudonym	Not Addressed	Not Addressed	Voting
Lo et al. (2009)	Decentralized	Summation	Not Addressed	Not Addressed	Not Addressed	Confidence Threshold
De Paula (2010)	Decentralized	Discrete	Fixed Identity	Partially Addressed	Addressed	Voting

Table 1. *Cont.*

Author	Administration	Reputation Mechanism	Privacy	Robustness	Network Impact	Vehicular Decision
Ding et al. (2010)	Decentralized	Fuzzy	Fixed Identity	Not Addressed	Not Addressed	Fuzzy
Huang (2011)	Decentralized	Not Addressed	Pseudonym	Partially Addressed	Not Addressed	Data Centered
Marmol et al. (2011)	Decentralized	Summation	Not Addressed	Partially Addressed	Not Addressed	Confidence Threshold
Jalali (2011)	Decentralized	Fuzzy	Not Addressed	Not Addressed	Not Addressed	Confidence Threshold
Fernandes (2013)	Decentralized	Bayesian Beta	Fixed Identity	Not Addressed	Addressed	Voting
Yang (2013)	Decentralized	Summation Similarity	Fixed Identity	Not Addressed	Not Addressed	Confidence Threshold
Park et al. (2011)	Centralized	Summation	Fixed Identity	Partially Addressed	Not Addressed	Not Addressed
Li et al. (2012)	Centralized	Summation	Pseudonym	Addressed	Addressed	Reputation Level
Liao et al. (2013)	Centralized	Probabilistic Bayesian	Fixed Identity	Not Addressed	Not Addressed	Confidence Threshold
Mühlbauer (2018)	Centralized	Summation or Probabilistic	Pseudonym	Addressed	Addressed	High Reputation or Voting

However, most research that does not deal with reputation systems adopts privacy mechanisms using pseudonyms and short-term certificates. A comparison of 41 schemas of information security for VANETs is described in [26], focusing mainly on authentication mechanisms and privacy protection. The authors identified several deficiencies in a significant portion of the considered works, such as mechanisms that may not coexist due to the level of differences between the concepts adopted, lack of clarification with respect to the assumptions made, failure to consider key issues and developing standards, and focus on point solutions rather than a holistic approach to vehicle networks.

There is a need to establish a set of common parameters of security and privacy services, considering reliability and interoperability. Thus, the Intelligent Transport Systems services can coexist in a single vehicular environment. Unlike most of the related works, the system proposed in this paper is aligned with this concept of a holistic approach without adopting mechanisms that cannot coexist on the concepts and standards currently under development for VANETs.

3. Proposed System

3.1. System Assumptions

The basic architecture of VANETs (Figure 1) involves vehicles equipped with processing modules and wireless communication called OBU (Onboard Unit); static communications infrastructure units called RSU (Road Side Unit); Governmental Transportation Authority (GTA); Certification Authority (CA) and the Central Control of Traffic Operation (CCO). VANETs require interoperability between different manufacturers and countries, demanding architecture and standardization efforts in the various layers of communication protocols and in the applications itself. As described in [27], the ISO/TC 204 working group is responsible for ISO's work (International Standards Organization) for ITS (Intelligent Transportation System). The American standard for vehicular networks is called IEEE 1609 WAVE (Wireless Access in Vehicular Environments). Among them IEEE1609.2 is the standard which specifies security of processing and message format, dealing with authentication and encryption issues.

The proposed system is aligned with these standards under development and the main experimental design of VANETs [8]. It has a hybrid characteristic of operation, which enables the use of the infrastructure available for the intermittent communication vehicle-to-infrastructure (V2I). This alignment allows for assumptions to avoid hardware or specific infrastructure for the reputation system so that it can be incorporated in the architecture envisaged for vehicular networks. The system requires the use of a vehicular public key Infrastructure (VPKI) [28], where each vehicle and RSU

has a unique identifier (ID), a pair of public/private key and long-term certificate assigned by the manufacturer and agreed with a certification authority (CA). In addition to the long-term identification, each vehicle generates a set of short-term private/public key and sends them securely to the CA. This CA signs the short-term keys and generates a set of pseudonyms for the vehicle. A hardware security module (HSM) in the vehicles has the function to the tamper proof storage of keys, certificates, and cryptographic processing.

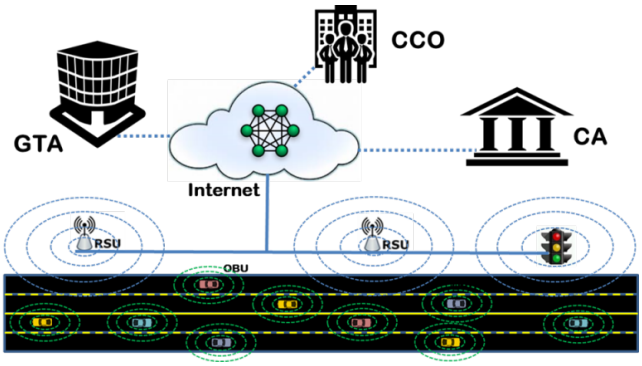


Figure 1. Typical architecture of a vehicular ad hoc network (VANET).

All messages transmitted by the vehicles must be digitally signed using a private key corresponding to the current short-term pseudonym (certified public key). The public key certificate must be attached to the message to attest the validity of the primary key. The receiver vehicle can check the authenticity of the message using the existing public key in the certificate, which in turn can be verified using the preinstalled public key of the certification authority. The system assumes the vehicles are equipped with a MVEDR module (Motor Vehicle Event Data Recorder), which is an electronic data recording device to store events and occurrences detected by sensors or processed by the ECU (Electronic Control Unit) modules [29].

3.2. Reputation System

The proposed system has the flexibility to work with several reputation calculation mechanisms. Some of them according to [2] are

- Simple Summation: obtained by adding the number of positive and negative reviews separately. Reputation is the difference between the total number of positives and negatives.
- Average of ratings: consists in calculating the average of all ratings.
- Average weighted by factors: based on the calculation of a weighted average of all ratings, considering factors such as the time of the evaluation, distance, context, role of the node in the network, reliability of nodes, etc.
- Bayesian system: consists in the calculation of the reputation by updating of statistical functions such as binomial beta or multinomial probability density of Dirichlet. The updated value is obtained by the combination of the previous value with the new evaluation.

A key point of the proposal is the concept of certified reputation [12] used in a VANET schema in [10]. However, contrary to this work, where neighboring vehicles have to confirm the validity of events, the proposed system performs validation centrally by the CCO authority. Due to this, events on the roads should be detected and consolidated in CCO entity with high precision, wide coverage of roads, and with a low false alarm rate. The scheme uses the MVEDR module to register the occurrence of a detected event that are sent to other nodes of the VANET, including digital signature and certificate that are part of the messages. Each vehicle carries its own level of reputation embedded in the short-term digital certificate issued by the CA entity, which is stored in a secure and inviolable manner in the HSM module.

3.3. Roles of the Authorities GTA, CA, and CCO

The governmental transportation authority (GTA) in Figure 1 is ultimately responsible for the planning, implementation, monitoring, management, and control of the vehicular networks, as well as delegation of tasks to the other entities CA and CCO. The CCO is responsible for monitoring and controlling traffic on roads and taking corrective action to deal with incidents. Figure 2 shows the relationship between these central entities and with the vehicles in the network. The governmental transportation authority (GTA) is responsible for granting the vehicle identification number (VIN) and the unique virtual identity of the vehicle, which are respectively printed in the chassis and stored in the non-volatile memory of the HSM module by the vehicle manufacturer. The central database of GTA has the registration of all vehicles and their virtual identities. The unique virtual identity is transmitted to a CA.

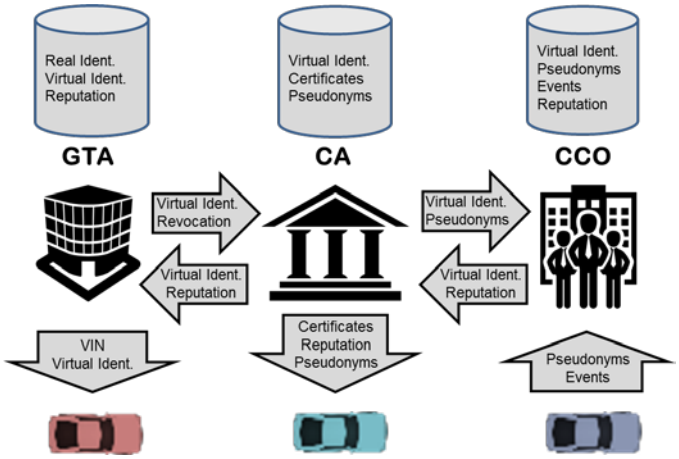


Figure 2. Relationships between entities in the system.

The initial level of reputation is established for each vehicle in the central database. Different strategies can be adopted: conservative (low initial reputation), neutral (middle initial reputation), and optimistic (high initial reputation). Information on the reputation of each vehicle is periodically transmitted to the GTA from the central mechanism of the CCO entity. The GTA is the only one that can decide and issue certificate revocation commands to the CA authorities.

The CCO entity periodically transmits reputation levels of the nodes to the CA entity, so incorporating them in the short-term digital certificates issued to each participating vehicle in the VANET network. The vehicles must have regular connections to a CA authority, albeit intermittently, to receive certificates and short-term pseudonyms for privacy protection purposes.

In the proposed system, before communicating with the CA entities, the vehicles need to previously connect to the CCO entity for transmission of relevant events recorded in their MVEDR module. This transmission must use the digital signature mechanism and symmetric encryption of the HSM module for secure communication against tampering or leakage of information.

The CA entity sends to the CCO entity the pseudonyms list of each vehicle, so the CCO can group the events linked to the pseudonyms reported by vehicles. The CCO entity communicates with the CA entity to inform the vehicles that previously provided their event logs to the CCO. When one vehicle does not communicate the events, it cannot receive new pseudonyms and short-term certificates and is soon unable to continue participating in the VANET network.

The CCO entity continuously receives information relating to the events on the roads under its jurisdiction and performs validation of the events reported by vehicles against their consolidated incident database. Confirmed events act in a way to increase the vehicular reputation, while events not confirmed decrease it. The CCO entity updates the vehicular reputation level by means of a reputation calculation mechanism, such as those described in Section 3.2.

This reputation level is transmitted to the CA entity linked to the Virtual Identification, so that the CA entity is able to incorporate the reputation level in the short-term digital certificates of the vehicles. If a vehicle does not report events to the CCO entity, a time-controlled reputation decay mechanism is applied. This will force the vehicle to update the reputation to continue to participate in the network or the certificate will be revoked.

3.4. Vehicular Decision Mechanism

The ephemeral and dynamic nature of VANETs hinders the establishment of trust between the vehicles because communication is often maintained only for a few s before being interrupted. Normally, there is not sufficient time to ask for a central database or other communication nodes about the reputation of the message issuer. Therefore, in the proposed system, trust between the vehicles can be obtained quickly and easily based on the certified vehicular reputation, which is stored and transported securely in the HSM module by the communication node itself.

The neighborhood vehicles in the radio range that are receiving messages from an event can check the validity of signatures by means of the digital certificates of the vehicles. If they are authenticated, the reputation of the vehicles attested by the CCO entity is extracted from the digital certificate, and the vehicle triggers a logical decision-making mechanism to assess the reliability of the received messages.

Raya [3] describes several types of mechanisms for vehicular logical decision: voting by the majority, choice of the message with the highest degree of reliability, weighted voting, Bayesian Inference, and use of the Dempster-Shafer theory. In the proposed system, we adapt these mechanisms to include the reputation, as appointed below: weighted voting by reputation level of the vehicles and choice of the message with the highest degree of vehicular reputation. The decision of the vehicle is performed by comparing the result calculated by the vehicular decision mechanism with a parameter called decision threshold.

4. Implementation of a Model

4.1. System Model

This section describes the implementation of a model of the proposed system. All the assumptions described in Section 3 are valid, even when they are not necessary or feasible for the simulations. As the certificate revocation decision process is outside the scope of this work, the simulation will always allow the redemption of the reputation of a malicious or anomalous node, without performing its definitive isolation of the network.

The simulations are related to road safety events (Notifications of Road Hazard) in two traffic scenarios: the Restricted Scenario and the Manhattan-Grid Scenario. In the first simulation stage, we use the Restricted Scenario and perform the measurements without the reputation mechanism. Then, we use two reputation mechanisms (Simple Summation and Bayesian Inference) to determine the mechanisms that presented the best results compared to the simulation without reputation system. The Simple Summation was chosen because is a mechanism commonly used in reputation systems, and Bayesian Inference was chosen due to its theoretical basis as described in [2]. In the second stage of simulations, we establish the Manhattan-Grid Scenario with the mechanisms of reputation and vehicular decision selected in the first stage.

The reputation system should be robust against information security attacks to the system itself. Some possible attacks described in [30] are

- Sybil attack: a single node attempts to create multiple identities or false pseudonyms to gain greater influence for their messages on the network.
- Newcomer attack: in case a new node can easily sign up to join the network, a malicious node can erase its past by registering as a new participant.
- Betrayal attack: before initiating its attack, the node behaves honestly in the network to achieve a reputation of high level.

- Inconsistency attack: the attacker tries to degrade the efficiency of the mechanism, by repeatedly switching its behavior between honest and dishonest.
- Bad-mouthing/Ballot Stuffing attack: nodes can provide intentionally incorrect ratings on other nodes in a positive or negative way, trying to influence their reputation on the network.
- Collusion attack: a group of nodes act cooperatively to create fake messages or influence the reputation of other nodes.

4.2. Description of the Restricted Scenario

This scenario aims to restrict vehicle movements and enable focus on the evaluation and comparison of reputation and decision-making mechanisms. The two mechanisms considered for the reputation calculation are Simple Summation and Bayesian Inference. The Bayesian Inference reputation mechanism was implemented with longevity function, allowing for the parameterization of the amount of stored historical data about the events reported by vehicles.

As illustrated in Figure 3, the Restricted Scenario consists of two possible routes: the short route #1 (800 m) and long route #2 (1200 m). Each route consists of single lane roads and one-way traffic. A journey is defined as a complete turn of a vehicle on Route 1 or 2. In the upper left corner of the scenario, there is a fixed station RSU, which represents the capacity to communicate with the CCO entity.

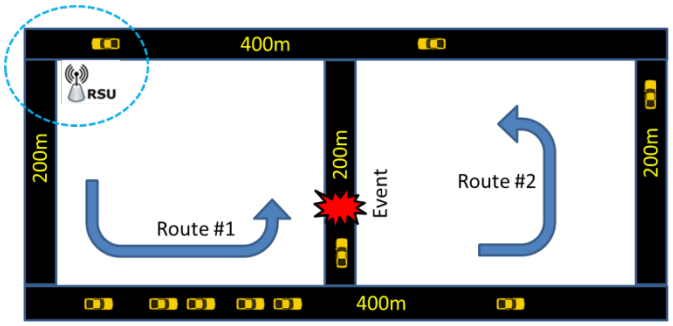


Figure 3. Restricted Scenario.

The simulation starts with 10 vehicles equipped with OBU modules in counterclockwise direction traveling in normal conditions only in Route #2. Events or incidents are scheduled for periodic occurrences, causing vehicles to remain stopped for a configurable period of time. In this situation, the vehicles that receive messages from the occurrence of the events may decide to deviate to Route #1. After completing the journey, returning to the starting point in the upper left corner, the vehicle enters into communication range with the beacon signals from the RSU station. At this moment, the vehicle send all events recorded in the MVEDR module (incidents notices) to the RSU.

The RSU (representing the CCO entity) stores the event history of the vehicle and the reputation. The CCO calculates the new level of reputation according to the mechanism under study, having as premise of simulation, the consolidated knowledge of the events. Thereafter, the RSU transmits the calculated reputation level to the vehicle, which stores its own reputation for use in upcoming transmissions of messages to the other nodes participating in the network.

Other vehicles use their decision-making mechanisms for the acceptance or rejection of the messages according to the decision threshold previously parameterized in the system. After each round, the vehicles continuously start a new journey until the end of the simulation.

To simulate the Restricted Scenario, the variable factors and their levels are reputation mechanisms, vehicular decision mechanisms, and attack types, as defined in Table 2. In this scenario, malicious attacks or anomalies are scheduled to occur periodically and are caused by one of the nodes in the network.

Table 2. Factors and levels of the Restricted Scenario.

Factor/Level	0	1	2	3	4
Reputation Mechanism	Without Reputation	Without Reputation	Simple Summation	Bayesian Inference with Longevity	Bayesian Inference without Longevity
Decision Mechanism	Always Negative Decisions	Majority Voting	Highest Reputation Level	Weighted Voting by Reputation	Always Positive Decisions
Attack Types	------	Newcomer	Betrayal	Inconsistency	------

4.3. Description of the Manhattan-Grid Scenario

As illustrated in Figure 4, the Manhattan-Grid Scenario has 12 city blocks (50 m by 100 m) with two lanes each in two-way traffic. At the bottom, 100 m away from the blocks, there are two tracks of 400 m with two lanes each in two-way traffic, which are used for the vehicles to complete their journey cycles. To obtain more realistic behaviors of the vehicles, they can perform overtaking and lane changes, as the speed of each vehicle is the result of a normal distribution depending on the maximum speed of the lane.

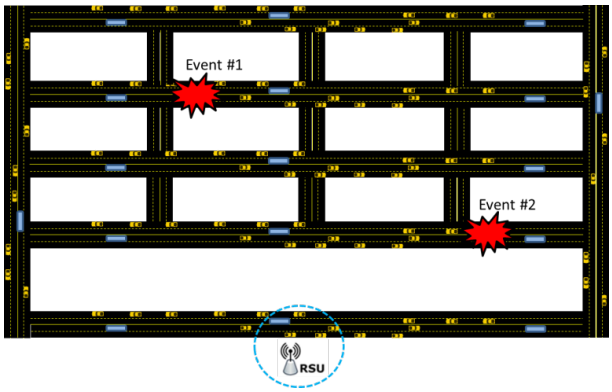


Figure 4. Manhattan-Grid Scenario.

The variable factors in the Manhattan-Grid Scenario are the quantity of malicious/anomalous nodes, the vehicular density, and types of attack defined in Table 3.

Table 3. Factors and levels of the Manhattan-Grid Scenario.

Factor/Level	1	2	3
Malicious Nodes	10%	30%	50%
Vehicular Density	20 vehicles	60 vehicles	100 vehicles
Attack Types	Newcomer	Betrayal	Inconsistency

4.4. Reputation and Decision Mechanism

In the scheme proposed in this work, we can use several mechanisms for calculating the reputation of nodes and event consolidation on the roads. The reputation level calculated by the central mechanism of the CCO entity for each vehicle can vary in the range 0–10, with 10 being the highest reputation value.

For the Simple Summation, the CCO entity needs only to keep the last registry of the calculated reputation for each node. Upon receiving an event notification message, the CCO entity checks its plausibility, and depending on the outcome of this verification, increases or decreases in one unit the reputation level of the vehicle.

Bayesian Inference is used according to the Beta Reputation System from Jøsang and Ismail [31]. The CCO entity checks the plausibility of the events reported by vehicles, and based on the results of this

verification increases the positive feedback counter or the negative feedback counter. The reputation of the target entity can be estimated by the expected value of the Beta distribution probability. If the reputation system operates with estimates ranging in range 0–1, the expected value of reputation is calculated by equation

$$Rep(r_T^x, s_T^x) = E(\varphi(p|r_T^x, s_T^x)) = (r_T^x + 1)/(r_T^x + s_T^x + 2) \quad (1)$$

in which r_T^x and s_T^x, represent respectively the positive and negative feedbacks accumulated over the target entity T, supplied by an agent or collection of agents. Due to the longevity factor, the CCO entity needs to store the event consolidation history, at least, to the extent of this factor.

The vehicular decision mechanism is based on the calculation of a decision value and checking if it is greater than the parameterized decision threshold. If the value exceeds this threshold, the vehicle takes a positive decision in relation to the event concerned; otherwise, the vehicle takes a negative decision.

Upon receiving a vehicle-to-vehicle (V2V) message, the receiver stores the event information in a decision table. This begins a time countdown for decision-making. As new messages arrive from other nodes on the same event, the vehicle continues storing information in the decision table. When the previously parameterized time is achieved, the decision mechanism applies one of the following calculation formulas:

- Always Negative Decisions: the decision value will always be the lowest.
- Majority Voting: the decision value consists of the average of all recorded events that have been reported by other vehicles during the period of decision.
- Highest Reputation Level: the decision corresponds to the event reported by the vehicle with the highest reputation. If there is more than one vehicle with the highest reputation, the mechanism considers the average of them.
- Weighted Voting by Reputation: the decision value is calculated as the weighted average of the reputation and the event reported by each node during the period of decision.
- Always Positive decisions: the decision value will always be the highest.

4.5. Simulation Environment

For the simulations, we utilized the VEINS framework v3.0, which operates in conjunction with traffic simulator SUMO v0.21.0, event simulator OMNeTpp v4.4, and Wireless Extension MiXiM v2.3. Table 4 shows simulation parameters used in the traffic simulations.

Table 4. Traffic simulation parameters.

Parameter	Value
Vehicle Size—Cars	5 m
Vehicle Size—Bus, Trucks	10 m
Minimum Distance Between Vehicles	2 m
Maximum Acceleration	3 m/s^2
Maximum Deceleration	6 m/s^2
Velocity of Vehicles	12 m/s
Distribution Variation of Velocity	Normal
Sumo Speed Factor	1
Sumo Speed Deviation	0.5
Entry Probability of Cars	90%
Entry Probability of Bus, Trucks	10%

4.6. Metrics Definition

The purpose of a reputation system should be to achieve the best possible efficiency, i.e., provide the highest number of right decisions by the user entities. For this work is the performance of the

reputation system under malicious attacks or vehicle anomalies. Table 5 summarizes the possible outcomes of the decision-making mechanisms in relation to right and wrong decisions. In each measurement of the experiments, we collected the following metrics: TN, TP, FN, FP, number of wrong decisions (sum of FN and FP), and number of right decisions (sum of TN and TP).

Table 5. Results classification.

Results		**Event Occurrence**	
		Absence	**Presence**
Decision	Negative	True Negative (TN)	False Negative (FN)
	Positive	False Positive (FP)	True Positive (TP)

5. Performance Analysis

All the results have a 90% confidence interval and each experiment was repeated 30 times with random seeds.

5.1. Results of the Restricted Scenario

Experiments combinations of Table 2 for the Restricted Scenario are as follows:

- R0D0: without reputation and always negative decisions;
- R1D1: without reputation and majority voting;
- R2D2: Simple Summation and highest reputation level;
- R2D3: Simple Summation and weighted voting;
- R3D2: Bayesian Inference with longevity and highest reputation level;
- R3D3: Bayesian Inference with longevity and weighted voting;
- R4D3: Bayesian Inference without longevity and weighted voting;
- R0D4: without reputation and always positive decisions.

In the Newcomer attack type, the malicious node performs attacks as soon as it begins its operation in the network. In this simulation, the number of honest events is greater than the number of malicious or anomalous events. Figure 5 illustrates the evolution over simulation time of the reputation level of the nodes in the following conditions: Newcomer attack, Bayesian Inference mechanism with longevity factor, and decision by the highest reputation level (R3D2).

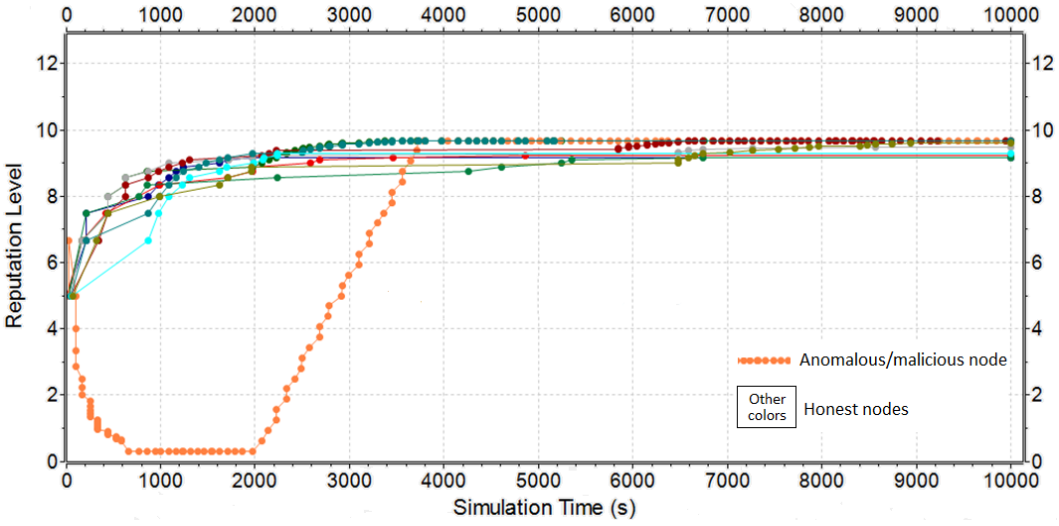


Figure 5. Reputation evolution for Newcomer attack—Restricted Scenario.

The malicious node performs the attacks of false event messages in the time interval between 0 and 2000 s. At the beginning of the simulation, the effect of the attacks causes the reputation fall of the malicious node. After the attack time, the node behaves honestly and there is a redemption phase. Figure 6 shows the results of the Newcomer attack in the Restricted Scenario for comparing the results of the experiments R0D0, R1D1, R2D2, R2D3, R3D2, R3D3, R4D3, and R0D4.

The R0D0 experiment is equivalent to a situation without the VANET. This experiment presents the worst results since the vehicles take only negative decisions, resulting in a high percentage of errors. The other extreme is the R0D4 experiment, where vehicles take only positive decisions, resulting in a high percentage of success due to the number of true positives but subject to attacks, as shown by the high number of false positives.

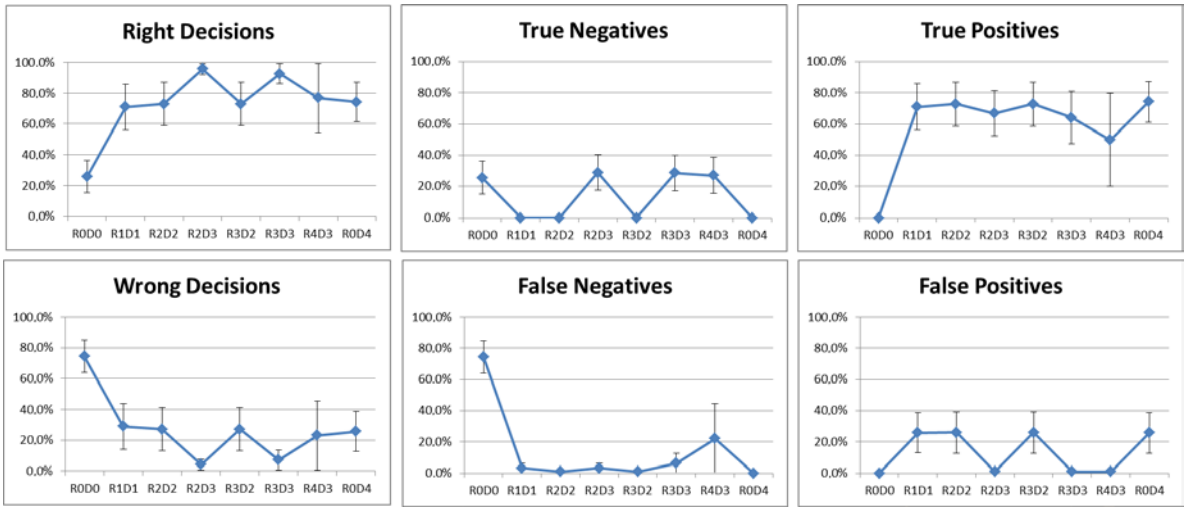


Figure 6. Newcomer attack for Restricted Scenario experiments.

The experiments R2D3 and R3D3 show the best results, using the weighted voting decision with reputation mechanisms Simple Summation and Bayesian Inference with low longevity factor. Due to the rapid response of the reputation mechanism to the events reported by vehicles, they virtually have no false positives related to attacks of the malicious node. Experiment R4D3 uses Bayesian Inference without longevity factor, which causes a slow recovery of the reputation of the malicious node. This factor increases the number of false negatives, thereby reducing the amount of right decisions in the simulation period.

In the Betrayal attack type, the malicious node initially presents honest behavior, obtaining good reputation level before starting the attacks. In this simulation, the false event message attacks occur in the time interval between 2000 and 4000 s. After this period, the malicious node sends true event messages, recovering its reputation according to the mechanism used in the experiment.

Figure 7 illustrates the evolution over simulation time of the reputation level of the nodes in the following conditions: Betrayal attack, Simple Summation, and decision by the highest reputation level. There is an initial increase of the reputation of the nodes, the reputation fall of the malicious node, and after the attack time, there is a redemption phase because the node behaves honestly again.

Figure 8 shows the results of the Betrayal attack in the Restricted Scenario for comparing the results of the experiments R0D0, R1D1, R2D2, R2D3, R3D2, R3D3, R4D3, and R0D4.

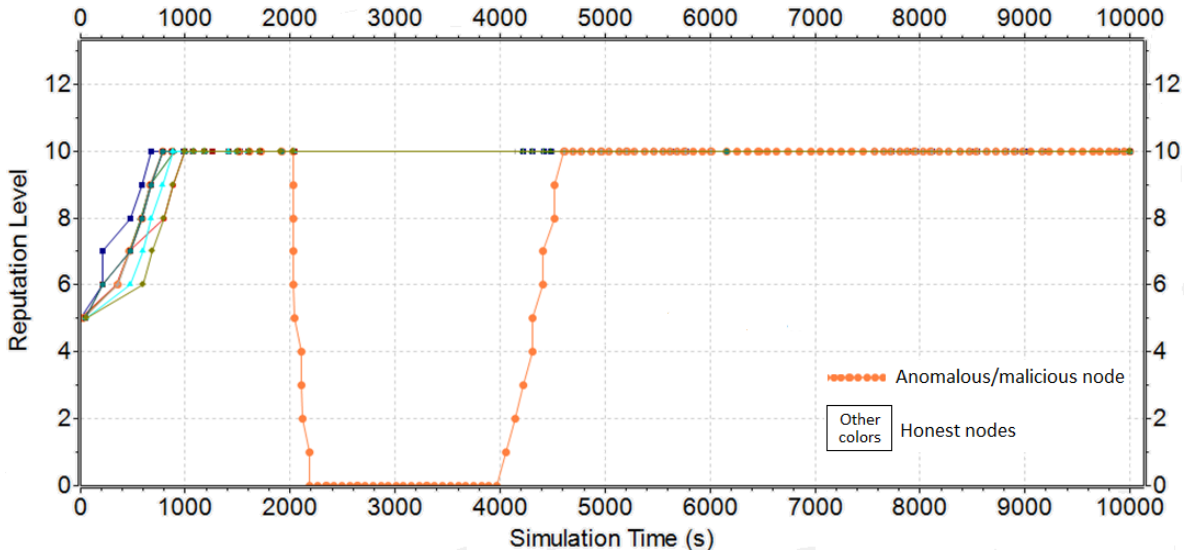


Figure 7. Reputation evolution for Betrayal attack—Restricted Scenario.

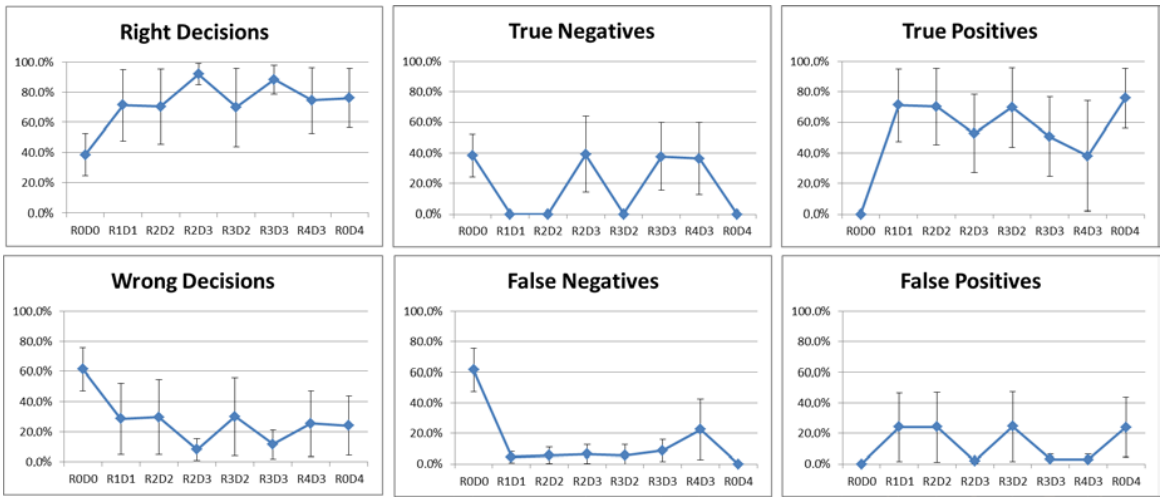


Figure 8. Betrayal attack for Restricted Scenario experiments.

In general, experiments with the Betrayal attack have a similar behavior to the Newcomer attack, especially R1D1, R2D2, and R3D2. In the experiments R2D3, R3D3, and R4D3, because of the weighted voting mechanism, the interaction with the true messages of the honest nodes caused a difference between Newcomer and Betrayal attacks. R2D3 and R3D3 experiments again present the best results.

In the Inconsistency attack type, the malicious node alternately sends true and false messages. Attacks start at simulation time 2000 and are held until the end of the simulation. This creates longer attack situations than the Newcomer and Betrayal experiments.

Figure 9 shows the evolution over simulation time of the reputation level of the nodes in the following conditions: Inconsistency attack, Simple Summation, and weighted voting by reputation. There is an initial increase of the reputation of the nodes; the reduction of reputation of the malicious node and its maintenance at a low level during the attack until the end of the simulation.

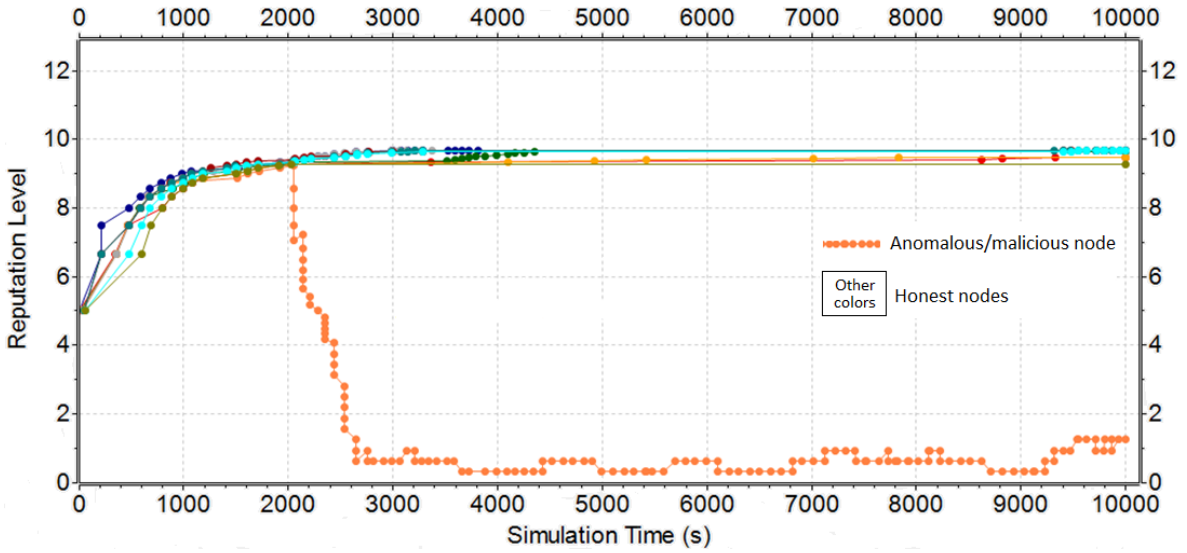


Figure 9. Reputation evolution for Inconsistency attack—Restricted Scenario.

The results of the Inconsistency attack in the Restricted Scenario are shown in Figure 10 for comparing the results of the experiments: R0D0, R1D1, R2D2, R2D3, R3D2, R3D3, R4D3, and R0D4. The experiments R1D1, R2D2, and R3D2 obtained a high number of false positives, therefore, vulnerable to this type of attack. Reflecting the higher number of false messages in the simulation compared to previous attacks, R2D3, R3D3, and R4D3 had a significant reduction in true positives to a level around 20%. Unlike other combinations of reputation and decision mechanisms, even when subjected to intense Inconsistency attack, the combinations R2D3, R3D3, and R4D3 continued to perform well, keeping right decisions close to 80% from the total.

Figure 10. Inconsistency attack for Restricted Scenario experiments.

The absence of vehicular decision-making mechanisms (R0D0 and R0D4) makes the network vulnerable to the simulated attacks. R1D1 shows unsatisfactory results due to the lack of reputation information in the voting process, becoming vulnerable when most messages are false or delivered by a single malicious node. The use of a reputation mechanism improves the system robustness. However, it should be used in combination with a suitable decision mechanism, as shown by the experiments R2D2 and R3D2. In these experiments involving the highest reputation level, the results were not

satisfactory since an attacker node may have low reputation, but still be the highest reputation received by other nodes.

Considering the robustness against the three attacks of the previous section, the experiments R2D3, R3D3 and R4D3 presented the best results. Regarding the mechanism of reputation calculation, the results indicate the Simple Summation reaches a higher level of right decisions than the Bayesian Inference. Due to the achieved performance, the combination R2D3 (reputation mechanism Simple Summation and decision weighted voting by reputation) was chosen for the Manhattan-Grid Scenario.

5.2. Results of the Manhattan-Grid Scenario

Experiments combinations of Table 3 for the Manhattan-Grid Scenario are as follows:

- D1M1: low density and 10% of malicious nodes;
- D1M2: low density and 30% of malicious nodes;
- D1M3: low density and 50% of malicious nodes;
- D2M1: medium density and 10% of malicious nodes;
- D2M2: medium density and 30% of malicious nodes;
- D2M3: medium density and 50% of malicious nodes;
- D3M1: high density and 10% of malicious nodes;
- D3M2: high density and 30% of malicious nodes;
- D3M3: high density and 50% of malicious nodes.

Figure 11 shows the evolution over simulation time of the reputation level in the D2M2 experiment under Newcomer attack in the Manhattan-Grid Scenario. In this simulation, attacks or anomalies occur in the time interval between 0 and 1000 s, where we can observe the reputation fall of the malicious or anomalous nodes. The redemption occurs predominantly in the time period between 2000 and 3000 s.

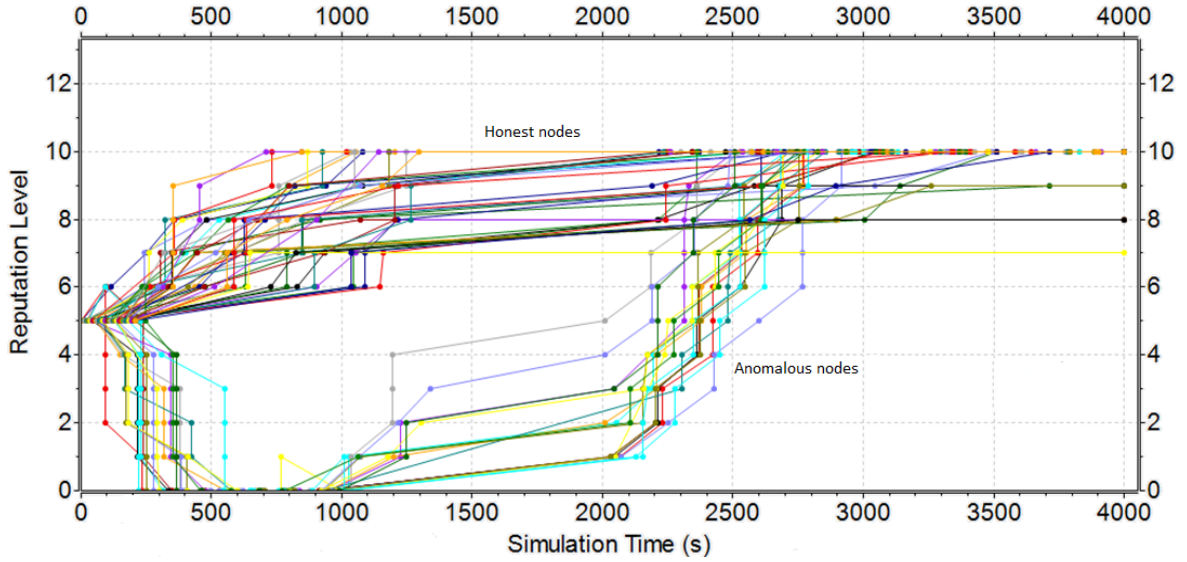


Figure 11. Reputation evolution for Newcomer attack—Manhattan-Grid Scenario.

Figure 12 shows the results of the Newcomer attack. The higher the density of the vehicles, the greater is the number of true positives, because more real traffic congestion events occur. Conversely, the percentage of true negatives is more significant in low vehicular density scenarios. The increase in malicious or anomalous nodes causes a decrease in right decisions.

Figure 12. Newcomer attack for Manhattan-Grid Scenario experiments.

Figure 13 shows the evolution over simulation time of the reputation level of the nodes in the D2M2 experiment under Betrayal attack in the Manhattan-Grid Scenario. In this simulation, attacks or anomalies occur in the time interval between 1500 and 2500 s, where we can observe the reputation fall of the malicious or anomalous nodes. The redemption occurs predominantly in the time period between 2500 and 3500 s.

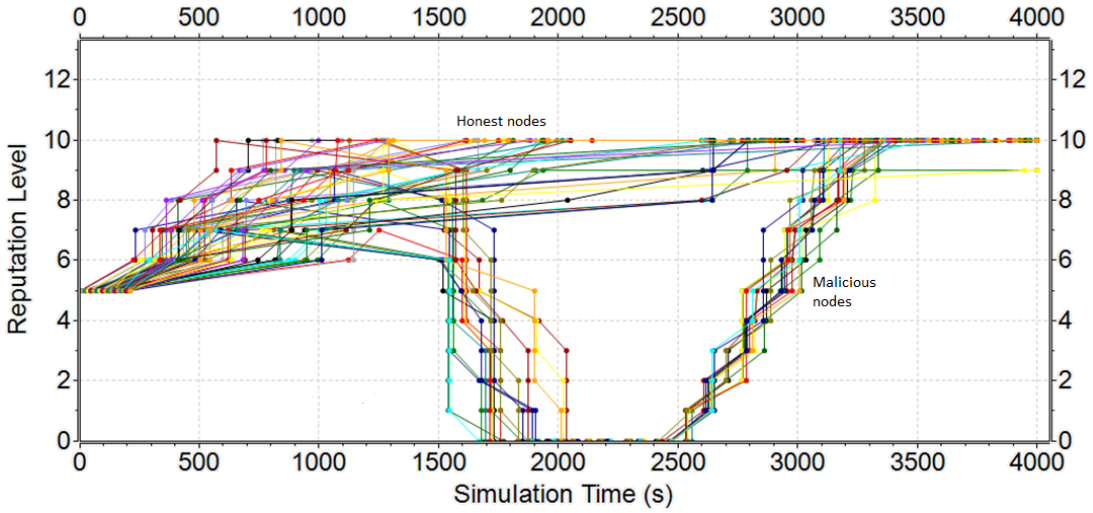


Figure 13. Reputation evolution—Betrayal attack—Manhattan-Grid Scenario.

The results of the Betrayal attack in the Manhattan-Grid Scenario are shown in Figure 14. In Betrayal attack, similar to Newcomer attack, increasing the vehicular density the number of correct decisions increases, while the increase of malicious or anomalous nodes increases the number of wrong decisions.

Figure 15 shows the evolution over simulation time of the reputation level of the nodes in the D2M2 experiment under Inconsistency attack in the Manhattan-Grid Scenario.

In this simulation, attacks or anomalies occur in the time interval between 2000 and 3000 s. At the same time, these nodes send true messages, trying to confuse the reputation system by inconsistent behavior. Due to the resilience of the mechanism, the reputation was kept in low value without significant fluctuation during the attack period or anomaly. Figure 16 presents the results of the Inconsistency attack in the Manhattan-Grid Scenario.

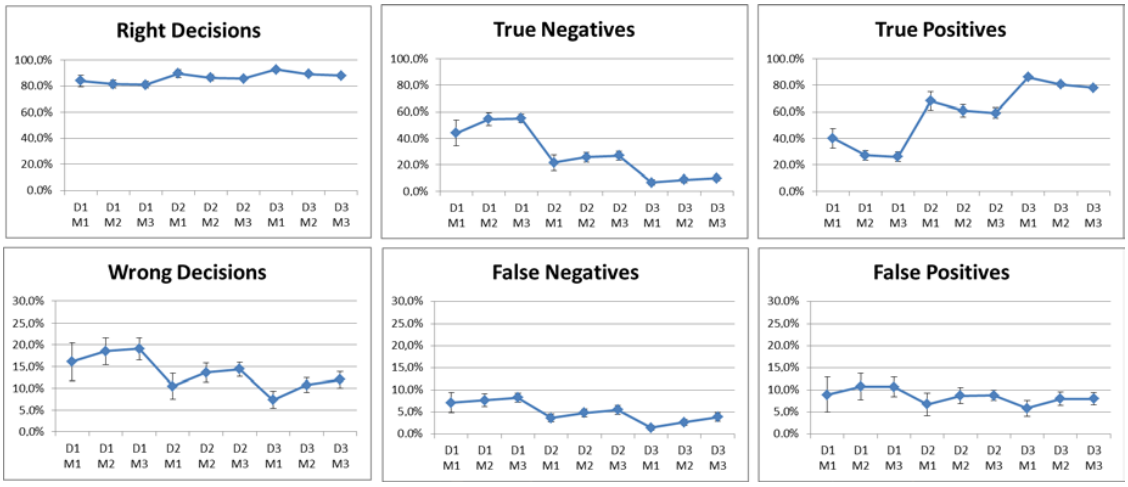


Figure 14. Betrayal attack for Manhattan-Grid Scenario experiments.

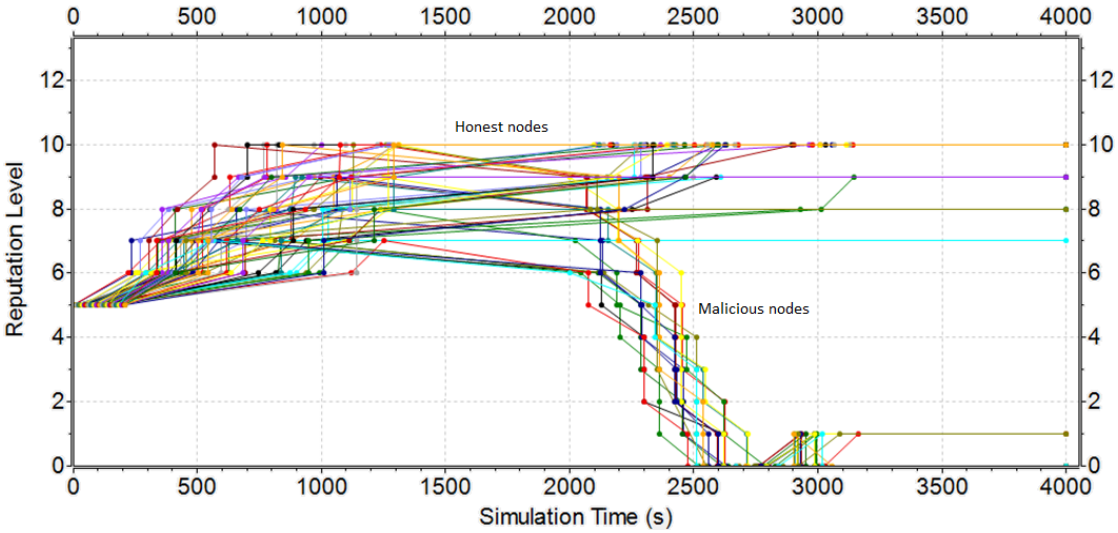


Figure 15. Reputation Evolution for Inconsistency attack—Manhattan-Grid Scenario.

Figure 16. Inconsistency attack for Manhattan-Grid Scenario Experiments.

In the Inconsistency attack, similarly to Newcomer and Betrayal attacks, the increased vehicular density increments the number of correct decisions, while the increase in the number of malicious or anomalous nodes increases the number of wrong decisions.

The comparison of the graphs of Figures 12, 14 and 16 shows the behavior of the reputation system was similar for the three types of attacks studied. The performance presented by the reputation system at the Manhattan-Grid Scenario in conditions of a sparse or congested network, variable number of malicious nodes, and with different types of attacks was consistent, with a range of right decisions between 80% and 90% of the total decisions in the VANET.

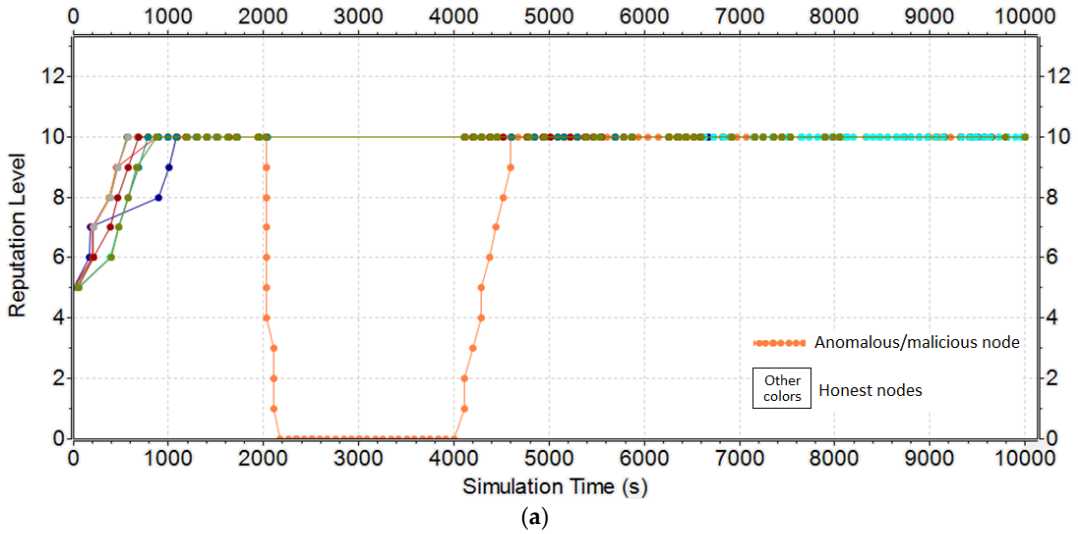
5.3. Response of the Reputation Mechanisms

This section presents a comparison of the response of the reputation system mechanisms: Simple Summation (R2), Bayesian Inference with low longevity factor (R3) and without longevity factor (R4).

Figure 17a shows the Simple Summation presents the most agile response to events reported by vehicles. After the report of only 10 events to the CCO entity, the scheme achieves an amplitude level variation of 10 in the reputation. For the simulation time used, this mechanism showed the best results. Figure 17b corresponds to the Bayesian Inference with low factor longevity, that is, the CCO entity considers only the last 30 events reported by vehicles to calculate the reputation of the nodes. This scheme also delivers good results in the proposed scenario, although not as fast as the previous mechanism. Figure 17c shows the Bayesian Inference mechanism without longevity factor, i.e., the CCO entity considers all events reported by the vehicles along the simulation time. This is a mechanism of slower response, which may be desirable depending on the scenario considered.

In both graphics of Bayesian Inference, we can observe the fall of the reputation level is faster than its recovery. This feature can be interesting for robustness against various types of attacks on reputation systems.

Figure 18 shows the influence of the reputation mechanism on the evolution of right decisions during the simulation time, taking as an example a measurement of R3D3 experiment. As the reputation of the malicious or anomalous node is high at the start of the attacks, a plateau in the right decisions by the neighborhood nodes and an increase in wrong decisions occurs at simulation time 2000 s.



(**a**)

Figure 17. *Cont.*

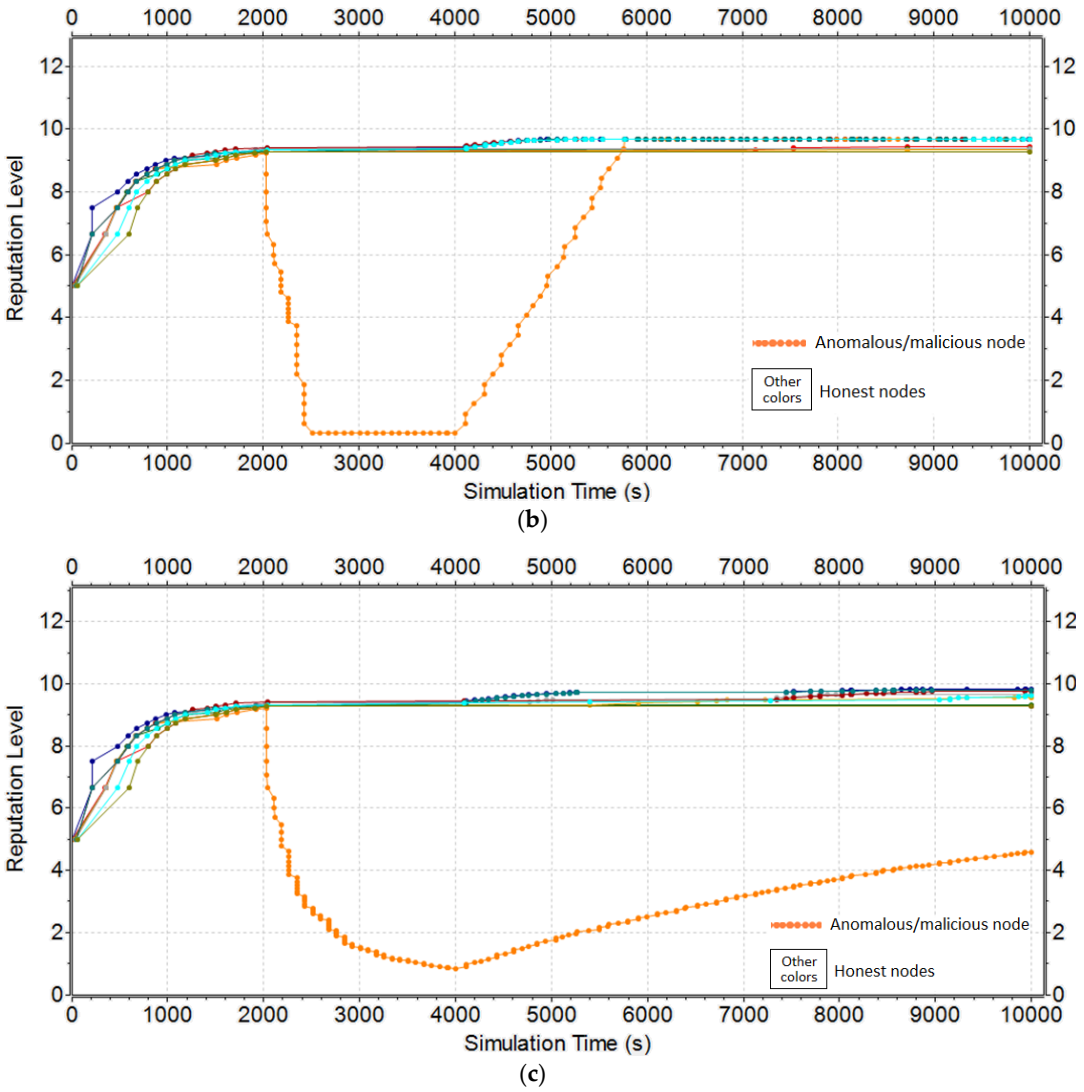


Figure 17. (**a**) Simple Summation mechanism, (**b**) Bayesian Inference mechanism with longevity factor, and (**c**) Bayesian Inference mechanism without longevity factor.

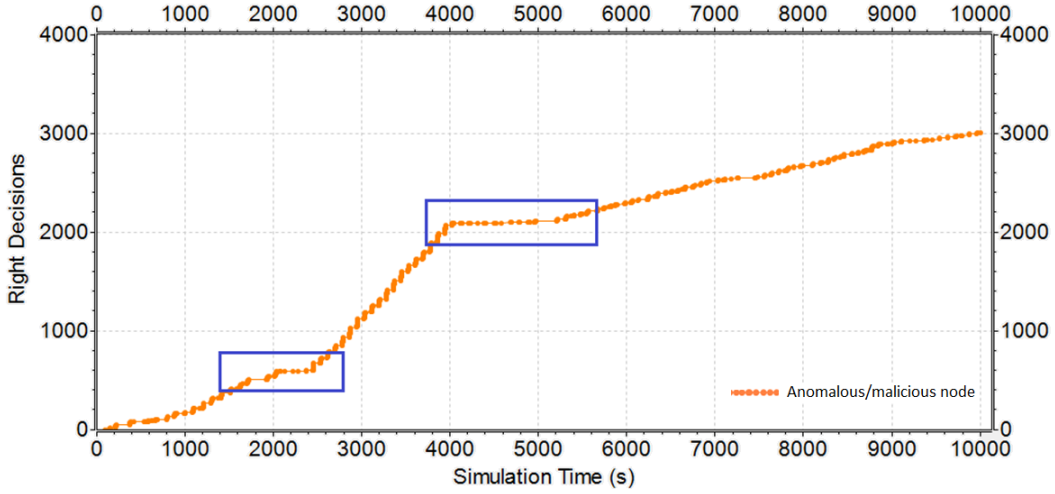


Figure 18. Evolution of right decisions.

The gradual decline in reputation results in decision values below the parameterized threshold, causing vehicles to take right decisions again, even when receiving false messages. After the attack period, the malicious or anomalous node resumes honest behavior, gradually increasing its reputation. However, due to its low reputation, there is a new plateau at 4000 s until the reputation of messages results in decision values above the decision threshold. At this point, the right decisions of the neighborhood vehicles increase again.

6. Conclusions

Reputation systems have been proposed for use in P2P systems, MANETs, and more recently in VANETs. Despite being an essential mechanism for information security in mobile and highly dynamic networks, a reputation system is not yet a consolidated mechanism, and it has not been considered in standards of vehicular networks currently under development. The application of reputation in mobile networks and in the Internet of Things is a complex challenge that can be overcome when the entities carry their own certified reputation attributed to them by a trusted authority, what could be named Bring Your Own Reputation (BYOR).

The research of this article uses this concept and proposes a centralized reputation mechanism for VANETs, which is aligned with the evolving standards, trends, and experiments of the major projects in the area. The results presented show the feasibility and tolerance to delays of the system without the need for permanent communication by the vehicles, as they carry their own reputation. Furthermore, the proposed system presents no difficulties to cope with pseudonyms for privacy avoiding traceability by other vehicles.

Due to the complexity of the vehicular networks and the restrictions and limitations of the model simulations, there is a need for further studies, which will open opportunities to consolidate and improve the proposed system. The system considers only single-hop broadcast communications. However, more research is necessary to extend the reputation mechanism for the selection of routing nodes for multi-hop communications for data summarization and aggregation by areas or geographical zones.

Author Contributions: R.M. and J.H.K. conceived and designed the experiments; R.M. performed the experiments; R.M. and J.H.K. wrote the paper.

Funding: This research received no external funding.

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

References

1. Hartenstein, H.; Laberteaux, K.P. A Tutorial Survey on Vehicular Ad Hoc Networks. *IEEE Commun. Mag.* **2008**, *46*, 164–171. [CrossRef]
2. Jøsang, A. Trust and Reputation Systems. In *Foundations of Security Analysis and Design IV, FOSAD 2006/2007 Tutorial Lectures*, 1st ed.; Aldini, A., Gorrieri, R., Eds.; Springer: Bertinoro, Italy, 2007; Volume 4677, pp. 209–245, ISBN 978-3-642-23082-0.
3. Raya, M. Data-Centric Trust in Ephemeral Networks. Ph.D. Thesis, École Polytechnique Fédéral de Lausanne, Lausanne, Switzerland, June 2009.
4. Dötzer, F. Security Concepts for Robust and Highly Mobile Ad-Hoc Networks. Ph.D. Thesis, Institut für Informatik der Technischen Universität München, München, Germany, March 2008.
5. Hendrikx, F.; Bubendorfer, K.; Chard, R. Reputation Systems: A Survey and Taxonomy. *J. Parallel Distrib. Comp.* **2015**, *75*, 184–197. [CrossRef]
6. Raya, M.; Papadimitratos, P.; Gligor, V.; Hubaux, J. On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks. In Proceedings of the 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008.
7. Ding, Q.; Jiang, M.; Li, X.; Zhou, X. Reputation Management in Vehicular Ad Hoc Networks. In Proceedings of the International Conference on Multimedia Technology (ICMT), Ningbo, China, 29–31 October 2010; pp. 1–5.

8. Hartenstein, H.; Laberteaux, K.P. Past and Ongoing VANET Activities. In *VANET Vehicular Applications and Internetworking Technologies*, 1st ed.; Hartenstein, H., Laberteaux, K., Eds.; Wiley: Chichester, UK, 2010; Volume 3, pp. 1–4, ISBN 978-0-470-74056-9.
9. Park, S.; Aslam, B.; Zou, C. Long-term Reputation System for Vehicular Networking based on Vehicle's Daily Commute Routine. In Proceedings of the 8th Annual IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, 12–15 January 2018; pp. 426–441.
10. Li, Q.; Malip, A.; Martin, K.M.; Zhang, J. A Reputation-Based Announcement Scheme for VANETs. *IEEE Trans. Veh. Technol.* **2012**, *61*, 4095–4108.
11. Liao, C.; Chang, J.; Lee, I.; Venkatasubramanian, K. A Trust Model for Vehicular Network-Based Incident Reports. In Proceedings of the 5th IEEE International Symposium on Wireless Vehicular Communications WiVeC, Dresden, Germany, 2–3 June 2013; pp. 1–5.
12. Huynh, T.D.; Jennings, N.R.; Shadbolt, N.R. Certified Reputation: How an Agent Can Trust a Stranger. In Proceedings of the Fifth International Joint Conference on Autonomous Agents and Multiagent Systems, Hakodate, Japan, 8–12 May 2006; pp. 1217–1224.
13. Ostermaier, B.; Dötzer, F.; Strassberger, M. Enhancing the Security of Local Danger Warnings in VANETs—A Simulative Analysis of Voting Schemes. In Proceedings of the Second International Conference on Availability, Reliability and Security, Vienna, Austria, 10–13 April 2007; pp. 422–431.
14. Lo, N.W.; Tsai, H.C. A Reputation System for Traffic Safety Event on Vehicular Ad Hoc Networks. *EURASIP J. Wirel. Commun. Netw.* **2009**, *2009*. [CrossRef]
15. De Paula, W.P.; Oliveira, S.; Nogueira, J.M. Um Mecanismo de Reputação para Redes Veiculares Tolerantes a Atrasos e Desconexões. In Proceedings of the 28th Brazilian Symposium on Computer Networks and Distributed Systems (SBRC), Gramado, Brazil, 22 December 2009; pp. 1–8.
16. Huang, Z. On Reputation and Data-Centric Misbehavior Detection Mechanisms for VANET. Master's Thesis, University of Ottawa, Ottawa, ON, Canada, 2011.
17. Marmol, F.; Perez, G. TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *J. Netw. Comp. Appl.* **2012**, *35*, 934–941. [CrossRef]
18. Jalali, M.; Aghaee, N. A Fuzzy Reputation System in Vehicular Ad hoc Networks. In Proceedings of the 2nd International Conference on Ambient Systems, Networks and Technologies (ANT-2011)/the 8th International Conference on Mobile Web Information Systems (MobiWIS 2011), Niagara Falls, ON, Canada, 19–21 September 2011; pp. 951–956.
19. Fernandes, C.P.; Simas, I.; Wangham, M. Um Sistema de Reputação Descentralizado para Avaliar a Confiança dos Nós em Redes Veiculares. In Proceedings of the 13th Brazilian Symposium on Information and Computational Systems Security (SBSeg), Manaus, Brazil, 30 August 2013; pp. 1–8.
20. Yang, N.A. Similarity based Trust and Reputation Management Framework for VANETs. *Int. J. Fut. Gen. Commun. Netw.* **2013**, *6*, 25–34.
21. Marti, S.; Garcia-Molina, H. Identity Crisis: Anonymity vs. Reputation in P2P Systems. In Proceedings of the Third International Conference on Peer-to-Peer Computing, Linkoping, Sweden, 1–3 September 2003; pp. 134–141.
22. Seigneur, J.M.; Jensen, C.D. Trading Privacy for Trust. In Proceedings of the Second International Conference iTrust, Oxford, UK, 29 March–1 April 2004; pp. 93–107.
23. Yao, Y.; Ruohomaa, S.; Xu, F. Addressing Common Vulnerabilities of Reputation Systems for Electronic Commerce. *J. Theor. Appl. Electron. Commer. Res.* **2012**, *7*, 1–20. [CrossRef]
24. Dingledine, R.; Mathewson, N.; Syverson, P. Reputation in P2P Anonymity Systems. In Proceedings of the Workshop on Economics of Peer-to-Peer Systems, Berkeley, CA, USA, 5–6 June 2003.
25. Wang, Y.; Vassileva, J. Bayesian Network-Based Trust Model in Peer-to-Peer Networks. In Proceedings of the Second International Workshop Peers and Peer-to-Peer Computing, Melbourne, Australia, 14 July 2003; pp. 23–34.
26. De Fuentes, J.M.; Gonzalez-Manzano, L.; Gonzalez-Tablas, A.I.; Blasco, J. Security Models in Vehicular Ad Hoc Networks: A Survey. *IETE Tech. Rev.* **2013**, *31*, 47–64. [CrossRef]
27. Picone, M.; Busanelli, S.; Amoretti, M.; Zanichelli, F.; Ferrari, G. Standardization History and Open Issues. In *Advanced Technologies for Intelligent Transportation Systems*; Springer International Publishing: Basel, Switzerland, 2015; pp. 1–19.

28. Papadimitratos, P.; Buttyan, L.; Holczer, T.; Schoch, E.; Freudiger, J.; Raya, M.; Zhendong, M.; Kargl, F.; Kung, A.; Hubaux, J.P. Secure Vehicular Communication Systems: Design and Architecture. *IEEE Commun. Mag.* **2008**, *46*, 100–109. [CrossRef]
29. Young, C.P.; Chang, B.R.; Lin, J.J.; Fang, R.Y. Cooperative Colision Warning Based Highway Vehicle Accident Reconstruction. In Proceedings of the Eighth International Conference on Intelligent Systems Design and Applications, Kaohsiung, Taiwan, 26–28 November 2008; pp. 561–565.
30. Zhang, J. A Survey on Trust Management for VANETs. In Proceedings of the 2011 IEEE International Conference on Advanced Information Networking and Applications, Singapore, 22–25 March 2011; pp. 105–112.
31. Jøsang, A.; Ismail, R. The Beta Reputation System. In Proceedings of the 15th Bled Electronic Commerce Conference, Bled, Slovenia, 17–19 June 2002.