Kerrache, CA.; Lagraa, N.; Tavares De Araujo Cesariny Calafate, CM.; Cano Escribá, JC.; Manzoni, P. (2016). T-VNets: a novel Trust architecture for Vehicular Networks using the standardized messaging services of ETSI ITS. Computer Communications. 93:68-83. doi:10.1016/j.comcom.2016.05.013.

T-VNets: a novel Trust architecture for Vehicular Networks using the standardized messaging services of ETSI ITS

Chaker Abdelaziz Kerrache[a,*], Nasreddine Lagraa[a], Carlos T. Calafate[b], Juan-Carlos Cano[b], Pietro Manzoni[b]

[a] *Laboratoire d'Informatique et de Mathématiques, University of Laghouat, BP 37G, route de Ghardaia, Laghouat, Algeria*
[b] *Department of Computer Engineering, Universitat Politècnica de València, Camino de Vera, S/N, 46022 València, Spain*

Abstract

In this paper we propose a novel trust establishment architecture fully compliant with the ETSI ITS standard which takes advantage of the periodically exchanged beacons (i.e CAM) and event triggered messages (i.e DENM). Our solution, called T-VNets, allows estimating the traffic density, the trust among entities, as well as the dishonest nodes distribution within the network. In addition, by combining different trust metrics such as direct, indirect, event-based and RSU-based trust, T-VNets is able to eliminate dishonest nodes from all network operations while selecting the best paths to deliver legal data messages by taking advantage of the *link duration* concept. Since our solution is able to adapt to environments with or without roadside units (RSUs), it can perform adequately both in urban and highway scenarios. Simulation results evidence that our proposal is more efficient than other existing solutions, being able to sustain performance levels even in worst-case scenarios.

Keywords: Trust Management, Vehicular Ad-hoc Networks, ETSI ITS, Secure routing, Traffic estimation.

*Corresponding author
Email addresses: a.kerrache@mail.lagh-univ.dz (Chaker Abdelaziz Kerrache), n.lagraa@mail.lagh-univ.dz (Nasreddine Lagraa), calafate@disca.upv.es (Carlos T. Calafate), jucano@disca.upv.es (Juan-Carlos Cano), pmanzoni@disca.upv.es (Pietro Manzoni)

1. Introduction

Vehicular ad hoc networks (VANETs) have always been considered the keystone of Cooperative Intelligent Transportation Systems (C-ITS) [1]. Such communication systems have been deployed mainly to enhance safety on roads and to improve the passengers' comfort. Similarly to other open and dynamic networks, vehicular ad hoc networks suffer from different security threats [2], where the most dangerous ones are those targeting safe message generation and dissemination.

Many solutions have been proposed to ensure a secure and trusted delivery of such messages, as well as comfort messages. Nevertheless, finding a balanced tradeoff between security, efficiency, and network requirements remains an open challenge. Furthermore, existing solutions for securing vehicular communication can be divided into two categories: trust-based solutions and cryptography-based solutions, including the standardized 1609.2 and ETSI ITS security models [3, 4]. Cryptography-based solutions are known to provide excellent results for most security needs. However, all solutions in this category generally focus on outside attackers and introduce additional delays, limiting their usefulness in highly dynamic and delay sensitive networks such as VANETs. Concerning trust-based solutions for VANETs, which are based on economic science [5], they have attracted the research community mainly because this security solution can ensure highly trusted communications while promoting low-delay delivery without exhausting network resources.

Trust-based solutions for VANETs are generally classified into three categories: (i) entity-based, (ii) data-based, and (iii) hybrid solutions.

Entity-based works [6, 7, 8] attempt to eliminate dishonest nodes from all the network operations based on the exchanged recommendations between vehicles, which are piggybacked in existing messages or directly sent within new independent messages. In addition to the high time overhead introduced, works within this category do not take message quality into account, and assume that the

provider reputation is enough to secure communications, while in many cases honest nodes can also send or forward malicious messages [9, 10].

Since a stable reputation value for an unknown node is not feasible to achieve, few approaches in the data-based category [11, 12] assume that data quality is the only parameter allowing to secure all communications. These solutions typically compare exchanged data against a set of references representing data sent by an honest node. Obviously, this can represent an additional and costly delay when using a large database, and it cannot avoid Distributed Denial of Service (DDoS) attacks since attackers keep injecting packets resembling standard traffic.

Although hybrid techniques [13, 14, 15] try to revoke dishonest nodes and discard malicious data, they also suffer from the aforementioned shortcomings.

In parallel with all VANET enhancements proposed in the literature, tremendous efforts are also dedicated to standardize VANET communications. However, most of the existing solutions do not closely follow these standards.

In this paper, we propose a trust establishment scheme that uses C-ITS (Cooperative-Intelligent Transport Systems) messaging services CAM and DENM to carry the values of the necessary metrics in order to provide: (i) fast and trusted event message dissemination, (ii) continuous estimations of both traffic density and dishonest nodes' distribution within the network, and (iii) efficient techniques to revoke dishonest nodes in a collaborative manner. Our solution works transparently to the specific environment, being effective both in urban and freeway or highway scenarios, with or without RSU deployment. In addition, we propose a path selection technique which allows fast delivery of data messages via the shortest trusted path.

The rest of this paper is organized as follows: in section 2 we present the main existing trust-based solutions. In section 3 we provide an overview of our proposal. Section 4 details the proposed solution. Afterward, in section 5, we explain how the trust establishment can enhance the inter-vehicular communication data routing. In section 6 the simulation environment is described, and simulation results are discussed. Finally, some concluding remarks are provided

in section 7.

2. Related works

Trust models can be seen as decision-based reputation systems [16]. They have been inspired by economic science, and used afterward to enhance security in many other fields, especially in communication networks [17].

Many works have been proposed to provide trust management in VANETs, and they are usually classified into entity-based [6, 7, 8, 18], data-based [19, 11, 12] and hybrid [13, 20, 21, 22, 14, 15] models, depending on the solution target. In this section we describe the most recent and relevant works.

2.1. Entity-based trust models

Entity-based trust models aim at excluding dishonest nodes from all network operations, either temporarily or permanently. Most of the proposed works within this subset adopt a technique to gather recommendations from other nodes, usually by dividing vehicles on the road into different clusters orchestrated by a pre-selected clusterhead.

Haddadou et al. propose an approach inspired on the incentive model of banks [6]. It allows excluding malicious nodes based on a credit value, and this value can be increased or decreased following the behavior of the node in the network. However, it considers that the direct and indirect trusts are the same, and it does not take into account the specificities of each situation to differentiate between messages.

Another trust and reputation model was proposed by Yang [7]. In this work, messages are represented by a 4-tuple (identity, event type, latitude and longitude, event time), and the vehicle by a 3-tuple (identity, vehicle type, vehicle velocity). Similarity between nodes is computed based on the Euclidean distance, where each vehicle stores a weight called "direct experience-based reputation", that is related to the messages' producers, and another weight about recommendations from vehicles from which they received the same messages. Although

this scheme preserves a good events' message quality, it has some shortcomings since it only deals with event information. Moreover, the Euclidean distance cannot provide global information of similarities between two nodes. In addition, this scheme does not detail how to penalize nodes that have provided false recommendations. The number of received recommendations, and the reliability of the source of these recommendations, are a main concern as well.

Unlike [6, 7], Khan et al. [18] propose detecting dishonest nodes by computing a distrust level of nodes. This level increases with node misbehavior. Using the continuous observation of the neighborhood, every node sends a report about its untrusted neighbors to the clusterhead, and then to the trusted authority (TA), allowing to revoke nodes judged as untrusted. Nevertheless, authors did not provide enough details about the communication steps of this approach. In addition, this solution seems less effective than other existing solutions in terms of the overhead caused by node reports.

A different way to establish trust in VANETs was suggested by Jesudoss et al. [23]. They propose stimulating truth-telling and cooperation among VANET nodes through a Seller-Buyer scheme. Similarly to [24], they propose a clustering technique to reduce the communication overhead. They assign a reputation weight to all nodes participating in the clusterhead election and network control tasks by sharing their reports about the exchanged traffic. While showing good detection rates, this scheme does not respect reference trust metrics such as direct and indirect trust, and does not guarantee the privacy of vehicles. Moreover, high mobility levels can cause this scheme's performance to decrease considerably.

A solution focused on the routing process is proposed in [25]. It represents an attempt to secure the GyTAR routing protocol [26] by establishing trust among vehicles. To this end, authors propose an inter-cluster communication solution where the clusterhead is the only node responsible for evaluating the trust level of different peers (i.e vehicles). The main concern about this work is the way it deals with resource exhaustion by defining a threshold. If a node exceeds this threshold, it will be considered dishonest. However, there is neither

information about how clusterheads are selected, nor about how the threshold is adjusted. Moreover, this in-clusterhead centralization approach causes a high delay, and the dangers associated to a malicious clusterhead emerge.

In [27] authors proposed a social contribution-based technique to stimulate selfish nodes for being more cooperative. This solution is quite a hybridization of works [23] and [25] where trusted vehicles with a higher number of successfully routed messages are the preferred next forwarders. These vehicles can also be seen as nodes with a high message forwarding probability, as computed through the number of exchanged beacons and data messages. A betrayal attack can easily be launched in this case since communications are centralized around vehicles behaving legally at first. In addition, the problem with this approach is that the signal propagation model is not taken into account, thereby failing to consider basic urban environment conditions in their experiments. This means that this scheme cannot achieve the results shown when facing real environments.

The last scheme in the entity-based trust models category is represented by an intrusion detection mechanism for vehicular networks proposed in [28]. Based on a set of vehicles called guards, this technique tries to detect service-oriented attacks. Every guard node remains in promiscuous mode to identify misbehaving nodes within their guard zone; also, each guard cooperates with other guards for managing shared zones. Regular vehicles will be categorized into untrustworthy, uncertain, and trustworthy using predefined thresholds. Unfortunately, and similarly to all cluster-based solutions, this approach fails in the case of malicious guards.

2.2. Data-based trust models

In entity-based trust models the exclusion of dishonest nodes from any operation can lead to the disconnection problem. The latter occurs when there are large gaps between vehicles due to a low number of vehicles or obstacles, or due to node revocations because of an inappropriate dishonest or selfish behaviour. Since having a low vehicle density or obstacles cannot be prevented, the idea of filtering malicious messages without revoking theirs sources seems

worth considering in order to reduce the disconnection problem effect.

Golle et al. [19] propose a classical scheme similar to signature-based solutions. In this approach, any received message is compared with a model of non-malicious messages in VANETs maintained by all nodes. If no resemblance is signaled, then data will be dropped; otherwise, it will be forwarded. As a signature-based scheme, the main drawback of this approach is the construction of a global model for trustable communications in VANETs.

A data-based trust model for Ad-hoc ephemeral networks is proposed in [11], where the trust of any entity is fixed a priori depending on its role (e.g. $Trust(Police\ vehicles = 1;\ ordinary\ vehicles = 0.5)$). The model uses different trust metrics to determine the trust level of event reports. Then, it evaluates the evidences related to this event using Dempster-Shafer theory and Bayesian inference. Nevertheless, this approach achieves a good performance just in the case of non-redundant and abundant data, as required for the training phase. Moreover, in highly dynamic and open environments such as VANETs, fixing the trust level of entities represents another weakness of this approach, where a group of nodes can be controlled by a malicious entity to perform a colluding attack.

Another event-related solution is proposed in [29] where authors implement an intrusion-aware trust model based on three main steps: (i) computation of a confidence value for each message coming from a unique source; (ii) for all messages describing a same event, a trust value is calculated using the confidence information of step i; and (iii) accepting of rejecting the event message depending on its trust value. Despite the high accuracy of this approach, it introduces a high waiting delay, which is not acceptable when targeting VANET safety applications, and it cannot perform adequately in sparse scenarios.

Similarly to the three previous works, Gurung et al. propose an information-oriented trust model called "RMCU" [12] that also attempts to filter-out messages with low trust levels. This scheme consists of two components: (i) a message classification scheme, and (ii) an information-oriented trust model. Using the proposed message classification scheme, every vehicle can gather messages

describing a same event, and then divide them into two groups according to differences in their reports using a predefined threshold. This entire processing is done based on three metrics, which are content similarity, content conflict and routing path similarity. Finally, the information-oriented trust model determines which group of messages is effective, and then it allows discarding the opposite group. Unfortunately, this approach does not take into account the high mobility inherent to VANETs, and its time complexity is high. In addition, in the case of message sparsity, this scheme would not perform well.

2.3. Hybrid trust models

Trust models falling under this category aim at insuring reliable communication between nodes in the face of hostile nodes, as well as malicious messages. Most of the existing works adopt a clustering technique to minimize their communication overhead [13, 20, 15, 24, 30], but these centralized solutions always fail in the case of malicious clusterheads and under very dynamic urban scenarios.

Zhang et al. [13] propose a framework for message propagation and evaluation. In this approach, and to minimize the number of exchanged messages, authors adopt a clustering organization whereby messages are relayed only between cluster leaders. Upon receiving a message, a leader sends it to the cluster members to gather their opinions about the message. Finally, based on the collected opinions and the blacklist sent by the certification authority (CA), the leader can decide whether to relay the message. However, this scheme adds an important overhead to messages as it aggregates trust opinions and node signatures. It can be considered inefficient in the case of selecting a malicious cluster leader, achieving bad results in the presence of betrayal attacks.

TRIP [20], an infrastructure-based proposal supporting both trust and reputation in the scope of vehicular ad hoc networks, makes a classification of nodes into three different trust levels. In addition, authors associate a confidence level to each message. By combining node categories, message confidence and recommendations coming both from RSUs and nearby nodes, they compute a weight

called reputation score, which will be compared with three fuzzy sets (no trust, +/-trust, trust). If the weight is in the first set, the message will be rejected. If it is in the second one, the message will be accepted but not forwarded. Finally, if it is in the last set, the message is accepted and then forwarded. However, this model has some deficiencies associated to the number of recommendations required, and those situations where a fake set of recommendations is present; also, authors do not detail how to choose the initial weights (α, β, γ) concerning to direct previous experiences of nodes.

T-CLAIDS [14] is another work providing a trust-aware intrusion detection solution for VANETs. This solution takes into account the density, mobility and the vehicles' motion direction to perform an action, while maintaining a probability vector of all actions. This probability vector will be updated in the iterations that follow until convergence to a particular value is achieved, offering an approximate representation of a global knowledge about the environment. Unfortunately, even if this solution shows good results in the general case, it looks questionable in the case of unpredictable events. Also, the convergence time may be very long in sparse cases since it will be hard to gather all the information required to have a global view.

Sedjelmaci et al. [15] propose the use of three cooperative levels of intrusion detection to evaluate messages: (1) Local knowledge based intrusion detection in every vehicle; (2) Collaborative detection performed by the clusterheads; and (3) Global detection within the RSU. The latter is responsible for computing a trust level for each vehicle. The main weaknesses of this approach are: (i) the time needed for cluster creation and clusterhead election is excessive; (ii) in urban environments the assumption about stable clusters is not realistic; and (iii) in the absence of RSUs there is no trust and, hence, even if the IDS detects intrusions, there is no punishment for intruder nodes.

Bali and Kumar [24] propose a trust-based technique for secure cluster formation and data dissemination in VANETs. The proposal is based on two essential modules: sensing modules to gather information about vehicles traffic, and a cloud-based module responsible for computing vehicles' trustworthiness

depending on the gathered information. Despite the trusted cluster formation and maintenance, this scheme has many limitations. A deep explanation must be provided about the sensing module usefulness since its gathered information is already included within the periodically exchanged messages. In addition, this scheme seems more focused on highway scenarios since it is difficult to have stable clusters for long periods (about 140 seconds are required to create new clusters and select the new clustersheads, according to the paper).

A cooperation-based scheme for managing alert propagation in VANET is proposed in [30]. Authors define a typical communication model represented by a set of activity diagrams. This scheme is very similar to the work in [13], where the clusterhead forwards the alert message only if its cluster members agree about its validity, with the difference that decisions about message validity are taken by comparing them against an adequate activity diagram. Unfortunately, this solution inherits the same problems of [13].

In addition to the cluster-based trust establishment, fully distributed and hybrid trust models are available as well [31, 32, 33].

A trust-based scheme for message relaying was proposed in [31] based on a modular architecture, trying to deal with different kinds of messages, including control and safety ones, to ensure trusted and fast data delivery by only choosing trusted intermediate nodes as message relayers. Despite the obtained results evidence this scheme's efficiency, the performance levels achieved in urban environments significantly differ from those achieved in highways and freeways.

Haddadou et al. [32] propose a trust management scheme inspired on economic science. The scheme, called (DTM^2), has many features as it forces nodes to be helpful and cooperative within the network by establishing a communication price. This price will be high in the case of misbehaving nodes, thus limiting their participation in the network, while trustful nodes are rewarded. Despite extensive simulations, and the high performance levels achieved, a clear description of their adversary model should be provided in order to judge the performance under different types of attack, especially betrayal attacks where a node behaves legally for a short period of time to gain the trust of other nodes,

and then starts behaving illegally.

Unlike classical trust models, Rostamzadeh et al. [33] try to divide the map into different areas, and the traffic into three categories: safety, infotainment, and third party services, such as inter-taxi communication. Their proposal, called "FACT", is divided into two modules: admission and dissemination. In addition, the message source should be known by piggybacking the identities of all vehicles participating in the routing process. The admission module is responsible for analyzing the messages using the traffic category and the path's trust. If the degree of satisfaction is high, the dissemination module is responsible of selecting a trusted path for the message. Unfortunately, this solution adds a considerable overhead and processing delay. Moreover, authors do not provide information about security performance.

Overall, it is clear that existing works are not standard-compliant solutions and have different drawbacks, suffering from considerable overhead, computation delay, and security problems associated to clustering, among others. Also notice that most of them are specific to only one kind of information (safety or comfort), and they are dedicated to either urban or freeway scenarios. In addition, radio jamming DoS attacks are also among VANET's main threats. However, except for the work in [11] and our previous work [31], existing trust-based solutions did not consider this kind of adversary. Nevertheless, efficient lightweight solutions at the medium access control (MAC) layer have been proposed [34, 35, 36] to deal with such critical cases. Hence, we believe that existing trust-based solutions can be easily extended to deal with jamming DoS attacks through the use of any of the above MAC-based solutions.

Therefore, in this paper, we propose a trust establishment scheme based on the ETSI standard that can ensure a fast, distributed, and collaborative security framework supporting dishonest nodes' revocation, malicious data filtering, and DoS attack prevention. Moreover, we propose a real-time traffic estimation technique, and a novel procedure for routing messages.

Implementing our proposal makes T-VNets independent, scalable and able to operate in conjunction with any other communications protocol merely by

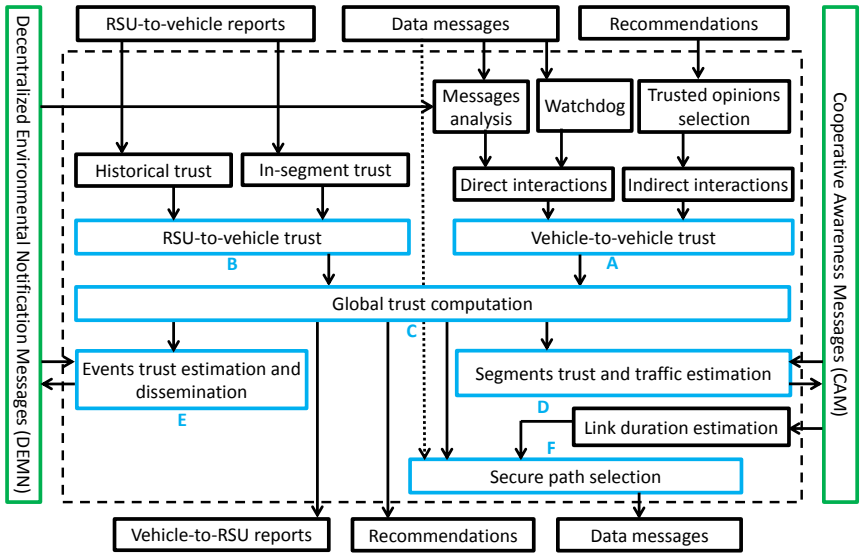

Figure 1: Proposed trust establishment architecture.

adding one or more of our solution's trust metrics to its main path scoring function, thereby achieving greater security and robustness.

3. T-VNets architecture

In this work we propose T-VNets, a solution that provides trust establishment over vehicular networks using ETSI ITS messaging services. Specifically, based on the information carried by the periodical *Cooperative Awareness Messages* (CAM) and the event-triggered *Decentralized Environmental Notification Messages* (DENM), T-VNets can provide an efficient and continuous evaluation of traffic, as well as the distribution of dishonest nodes within the network.

Figure 1 shows the trust establishment architecture defined by T-VNets. Based on the different pieces of information collected, global trust relations are built. We distinguish between two main kinds of trust: inter-vehicles trust, and RSUs-to-vehicles trust.

Nodes within the network can compute a trust value about the honesty level

associated to the different interactions. Moreover, RSUs can be considered as a trusted third authority from which nodes can receive both instant and historical behavior evaluations. The latter are called in-segment and historical RSU evaluations, and together are used to build trust between RSUs and vehicles. Our solution takes advantage of the existing message format introduced by the ETSI standard to estimate the events' credibility, as well as the level of traffic on the roads and the distribution of dishonest nodes. Finally, the aforementioned features allow our framework to choose the most reliable, secure and shortest path to deliver legal data messages.

T-VNets trust establishment process is based on different modules, as shown in figure 1. It starts by evaluating the direct interactions between vehicles. This phase involves two modules: (1) the message analysis module, which accounts for both the received messages quality and the reported events effectiveness, and (2) the watchdog module, which generates reports about the direct neighbours collaboration in the different network operations. Simultaneously, whenever a vehicle 'i' observes a behaviour change regarding another vehicle 'j', it broadcasts either a positive or a negative recommendation about vehicle 'j' taking as reference a previously defined honesty threshold, which means that recommendations are not requested, but instead are automatically broadcasted whenever a vehicle notices a positive or a negative behaviour change. The gathered recommendations about a vehicle 'j' will later be combined in order to compute an indirect trust evaluation for vehicle 'j'.

In parallel with the previous vehicle-to-vehicle trust evaluation, whenever a vehicle 'i' encounters an RSU it delivers a report about its neighbours behaviour, thus allowing the RSU to have a quasi-global view about all vehicles; this way, the RSU will generate evaluations about both recent and historical behaviours of vehicles called RSU-to-vehicle trust evaluation.

Afterward, both vehicle-to-vehicle and RSU-to-vehicle trusts are combined to compute a global trust evaluation for every neighbor 'j'. Such value will be carried by CAM messages, and used later on to enhance both data and event message delivery while respecting DENM message specifications.

In sections that follow, we start by detailing how trust among vehicles can be updated depending on both local knowledge and vehicle-to-vehicle recommendations. The module responsible for this task is the one associated with label 'A' in figure 1. The second part will be dedicated to explaining how the presence of an RSU within communication range can enhance the trust computation and prevent both coalition and platooning attacks, which is the task of module 'B'. Third, we detail how global trust evaluation is computed using the two previous processes (module 'C'). In the fourth and fifth sections, which refer to modules 'D' and 'E', we explain how T-VNets takes advantage of ETSI ITS standardized CAM and DENM messages to enhance the inter-vehicle trust establishment. Finally, module 'F' is the one responsible for the trusted path selection and data delivery.

3.1. Trust metrics

T-VNets employs different trust metrics like direct, indirect, event-related and RSU-based trust. Moreover, to take advantage of this variety of trust metrics, we propose a message forwarding scheme that is effective both in the presence and in the absence of RSUs, thereby providing a more flexible solution that is adaptable to different types of environments. In the following, the 8 used metrics are listed with the same order of use.

- *Qmsg(i, j)*: quality of messages; it is the data centric evaluation of a node i about messages sent by another node j during a period of time.
- *ETR(E, j)*: event's trust; it can be defined as the degree of belief associated to an event 'E' as reported by a node j.
- *WDR(i, j)*: watchdog continuous evaluation, where every node participates in surveying the network by analyzing the sending frequency of neighboring messages .
- *DTR(i, j)*: the direct trust evaluation upon an interaction between a pair of nodes (i, j). This metric is computed based on every node's local knowledge without external feedback.

- *ITR(i, j)*: unlike the direct trust evaluation, a node 'i' computes the indirect trust for another node 'j' based on the opinions of network nodes about this node 'j', instead of i's local knowledge.

- *SRSU(j)*: in-segment RSU evaluation is the evaluation of a roadside unit about the behavior of a vehicle j within its current segment.

- *HRSU(j)*: historical RSU evaluation, represents a global view about a the trust of a vehicle 'j' generated by the RSU using j's different in-segments evaluations.

- *GTR(i, j)*: the global trust evaluation given by a node i to another j based on its overall behavior. This metric is the combination of all used metrics.

3.2. Adversary model

In general, reputation and trust-based systems are susceptible to different types of attacks [2, 37]. However, in this paper, we focus on the active attacks listed below:

- False alert: this occurs when a selfish or dishonest vehicle triggers an alert about an nonexistent event.

- Message dropping attack: when a node does not collaborate in the message transmission process and behaves as a blackhole.

- Denial of service attack (DoS): we consider a resource exhaustion attack by sending messages at a high frequency.

- Coalition and platooning attacks: where a set of dishonest nodes (or a set of nodes controlled by a dishonest node) are moving together in order to avoid being detected, and to gain trust by providing similar reports about nonexistent events.

This means that our adversary can be: (i) A sender of malicious messages or regular messages injected at a high rate; (ii) A relay node that can act as

a blackhole or camouflages its illegal behavior by relaying packets through an untrusted path; or (iii) A coalition of senders and relays having illegal purposes.

4. Proposal details

For the sake of clarity, our proposal will be divided into five main parts, and it employs the notations listed in table 1. In addition, we will be using Figure 2 as reference since it summarizes our adversary model and the different elements of our proposal.

Table 1: Notations used.

Notation	Meaning
$GTR(i,j)$	Global TRust Evaluation given by i to j
$DTR(i,j)$	Direct interactions' TRust given by i to j
$ITR(i,j)$	Indirect (recommendation-based) TRust given by i to j
$HRSU(j)$	RSU's Historical trust evaluation of j
$SRSU(j)$	RSU's in-Segment trust evaluation of j
$ETR(E,j)$	TRust of the Event E reported by j
$Qmsg(i,j)$	Quality of the messages sent by j to i
$WDR(i,j)$	i's WatchDog Report about j's cooperation behavior
α	Honesty factor
β	Dishonesty factor
δ	Trust increment factor
μ	Trust decrement factor
RL	Role playing factor
ρ	Message credibility factor

In subsections 4.1 and 4.2 we describe how direct and indirect inter-vehicles trust (DTR, ITR) can be computed, as well as the calculation for in-segment and historical RSU-to-vehicles trust (SRSU, HRSU)and then, how these metrics are combined to compute the global trust evaluation (GTR).

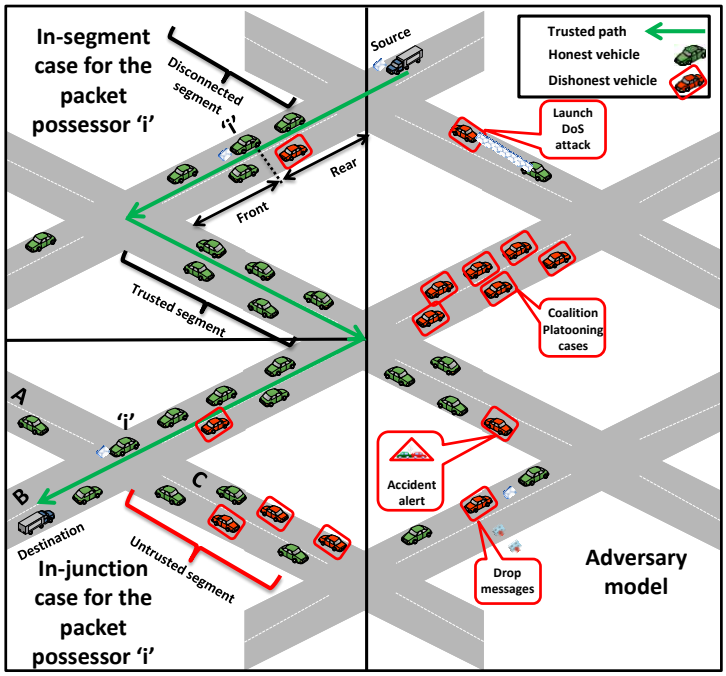

Figure 2: Adversary model, best path selection and routing different cases.

4.1. Vehicle-to-vehicle trust

Trust can be defined as a relation amoung entities based on the observation of historical interactions or recommendations [38]. Hence, the two main trust metrics are the direct interaction between every pair on nodes (i, j), and the recommendations coming to i about j. In the subsections below we describe how our solution maintains and updates the direct trust $DTR(i, j)$ and the indirect trust $ITR(i, j)$.

Figure 3 illustrates the used modules in this phase.

4.1.1. Direct trust (DTR)

In our case, DTR is the combination of the exchanged messages' quality (Qmsg) and a continuous report about the neighbors' degree of cooperation within the network using a watchdog technique (WDR), where every node remains in promiscuous mode and evaluates neighbor cooperation regarding network operations.

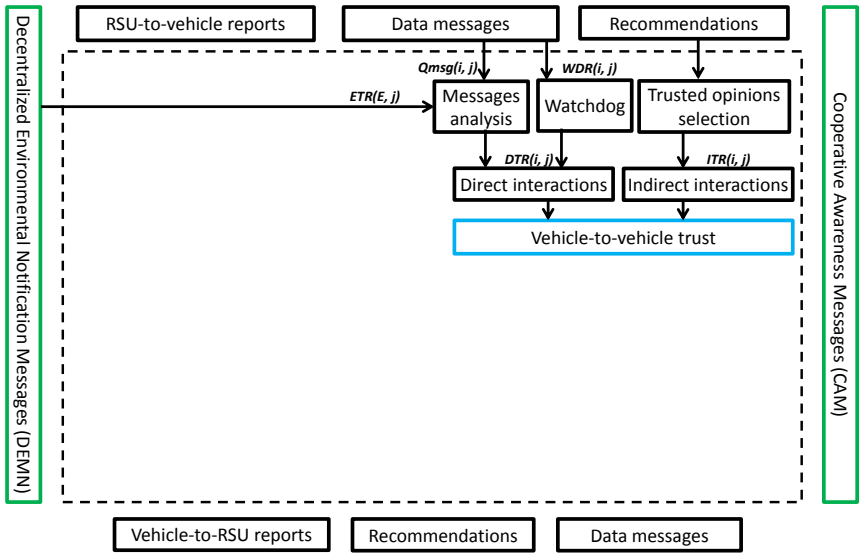

Figure 3: Vehicle-to-vehicle trust modules.

Similarly to all other trust metrics used, the intial 'DTR' value assigned by a node i to another node j is equal to 0.5, and it can vary from 0 to 1 depending on j's behavior according to equation 1.

$$DTR(i,j) = AVG\big[DTR(i,j), [(\beta \cdot Qmsg(i,j)) + (\alpha \cdot WDR(i,j))]\big] \quad (1)$$

Similarly to equation 6, α and β are two factors where $(\alpha + \beta = 1)$ and $(\beta > \alpha)$. They are used to give more importance to directly exchanged messages in a period of time compared to network collaborativity since we are evaluating the direct trust.

Moreover, every node evaluates its neighborhood and stores, for every neighbor, some information such as the Packet Drop Ratio (PDR) and the Packet Sending Ratio (PSR). In order to decide whether an ongoing attack is taking place, we define both a high (TH_h) and low (TH_l) traffic threshold. Then, we compare the PDR and the PSR against these thresholds, updating the watchdog report $WDR(i,j)$ according to algorithm 1:

Algorithm 1 Vehicles cooperation evaluation

INPUTS: PDR, PSR of a node j during a period of time.
OUTPUTS: Watchdog report updated.
if ($PDR(j) \geq TH_h$) **then** (DoS attack detected)
    $WDR(i, j) \leftarrow 0$;
else
    if ($PDR(j)/PSR(j) \leq TH_l$) **then** (blackhole attack detected)
        $WDR(i, j) \leftarrow WDR(i, j)\text{-}\mu$;
    end if
end if
End

In this algorithm notice that μ is the trust decrement factor.

For $Qmsg(i, j)$, since it is a direct interaction, all messages can be decrypted and analysed. Hence, a data trustiness value can be obtained. The global messages' trustiness in a period of time will be updated by i upon receiving a message from j using equation 2:

$$Qmsg(i,j) = AVG\Big[Qmsg(i,j), \frac{RL + \alpha \cdot \sum j's\_legal\_messages}{\beta \cdot \sum j's\_malicious\_messages + \alpha \cdot \sum j's\_legal\_messages}\Big] \tag{2}$$

'RL' is an aditional factor ($0 \leq RL \leq 0.5$) assigned to vehicles playing a specific role (police, ambulance, etc.); otherwise, $RL = 0$.

Dishonest behaviors (malicious messages) will cause the trust level to be multiplied by a factor β higher than the legal behavior factor α (legal messages), because one of the main features of trustfulness is being hard to gain but easy to lose ($\beta > \alpha$).

4.1.2. Indirect trust (ITR)

Indirect trust among vehicles is computed by gathering the vehicles' recommendations about each other. Usually, voting-based techniques have a bad impact on bandwidth usage. To avoid this unwelcome situation, all one-hop

neighbor recommendations will take into account only in the initial step; once the trust metrics are updated (after a small period of time), only trusted neighbor recommendations will be taken into consideration for indirect trust computation.

The indirect trust (ITR) given by a node i to another node j will be continuously updated following equation 3:

$$ITR(i,j) = \frac{\alpha \cdot \sum P\_recommendations\_about\_j}{\beta \cdot \sum N\_recommendations\_about\_j + \alpha \cdot \sum P\_recommendations\_about\_j} \quad (3)$$

Similarly to the previous cases, dishonest behaviors (negative recommendation) will cause the trust value computed to be multiplied by a factor β that is higher than the legal behavior factor α (positive recommendation), where $(\beta > \alpha)$.

4.2. RSU-to-vehicle trust

RSU deployment is considered a complex task under both freeway and urban scenarios since RSU coverage is often affected by the presence of obstacles. However, when communication is feasible, the RSU's quasi global view about the network can significantly enhance the trust establishment among vehicles.

Based on the periodic vehicle reports, an RSU can match the vehicles pseudo identity with their real identity since it can contact the certification authority. Hence, the RSUs can generate and forward some reports about the vehicles' historical behavior using their current pseudo-identities. In our case, we distinguish between two types of RSU reports: (i) RSU trust evaluation for the current road segment, and (ii) RSU trust evaluation for the global historical data. The main aim of this distinction is preventing coalition and platooning attacks. If we have a global idea about the past behavior of a node, we can combine it with information about its behavior within the current segment, and readily detect if it is participating in a coalition attack, or if it is part of a platoon composed of dishonest members sending positive reports about each other.

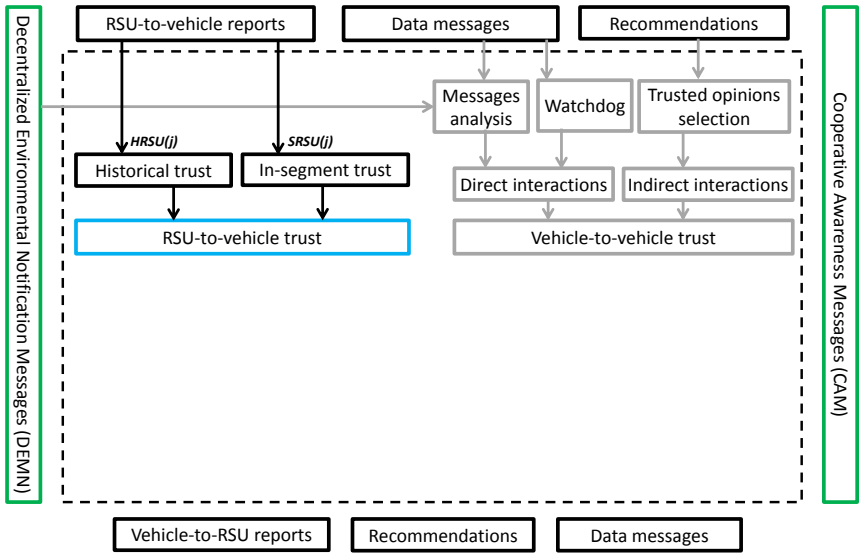

Figure 4: RSU-to-vehicle trust modules.

Figure 4 illustrates the used modules to compute both recent and historical RSU evaluations.

After filtering out reports coming from dishonest nodes, an RSU can compute a value representing the behavior of node j within its current road segment (SRSU(j)), and considering the time spent by the vehicle within that road segment. This time can be estimated using the segment's length and the vehicles' average speed, in addition to the traffic light waiting time. Equation 4 represents how the SRSU updates its information about a node j based on received reports about j:

$$SRSU(j) = \frac{\alpha \cdot \sum P\_reports\_about\_j}{\beta \cdot \sum N\_reports\_about\_j + \alpha \cdot \sum P\_reports\_about\_j} \tag{4}$$

In addition, based on the different in-segment trust evaluation reports received, an RSU can compute a global historical trust value concerning all nodes since it is usually connected to other RSUs. This global historical trust for a

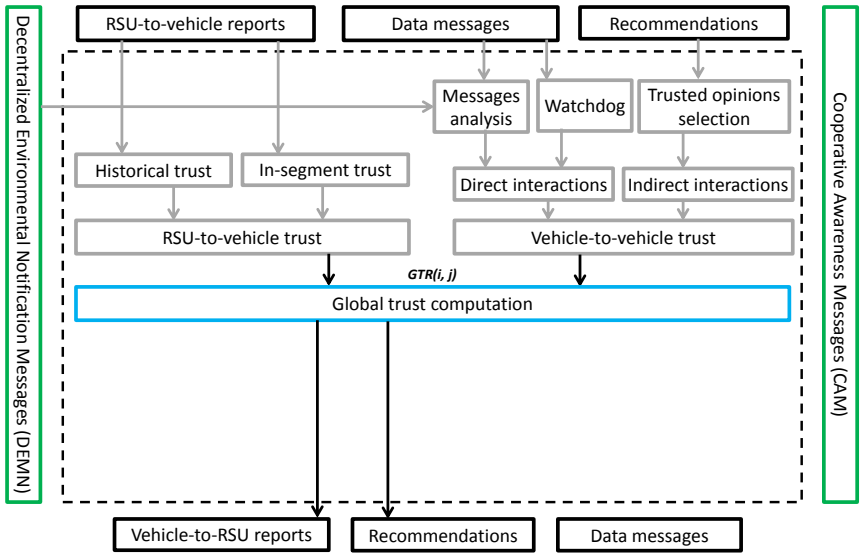

Figure 5: Global trust computation.

node j ($HRSU(j)$) is updated as follows:

$$HRSU(j) = AVG\Big[HRSU(j), \frac{\alpha \cdot \sum P\_SRSUs\_about\_j}{\beta \cdot \sum N\_SRSUs\_about\_j + \alpha \cdot \sum P\_SRSUs\_about\_j}\Big] \quad (5)$$

Factors α and β are also used in both equations 4 and 5 for the same purpose as in the previous equations. In addition, when an RSU is available, every node i sends a list containing the identities j of nodes assumed to be dishonest ($\forall$ j $/GTR(i,j) \leq danger\_value$). Otherwise, it broadcasts a positive or negative recommendation about j based on its trust value $GTR(i,j)$.

4.3. Global trust computation

The global trust evaluation uses both vehicle-to-vehicle and RSU-to-vehicle to evaluate a node j as illustrated in figure 5

Every node i can build a global trust view about any other node j in the presence, as well as in the absence, of an RSU within its communication range.

We call this global trust evaluation $GTR(i,j)$, and it will be updated periodically, although following a different procedure depending on whether nodes are in the presence of an RSU or not. The procedures are the following:

When located within an RSU's communication range, vehicles periodically receive both the historical (HRSU) and the in-segment (SRSU) behavioral trust of all nodes within the same segment. This allows every vehicle to have a clear idea about its direct and indirect neighborhood in order to prevent any kind of dishonesty. Equation 6 shows the global vehicle-to-vehicle trust updating process in the presence of an RSU:

$$GTR(i,j) = \beta \cdot \big[AVG[DTR(i,j),\ SRSU(j)]\big] + \alpha \cdot \big[AVG[ITR(i,j),\ HRSU(j)]\big] \tag{6}$$

To benefit from the global view provided by the RSU, we give more importance to the instant direct (DTR) and in-segment trust (SRSU) evaluations, instead of recommendations (ITR) and historical behaviour (HRSU). To this end, we employ factors α and β, with (α + β=1) and ($\beta > \alpha$).

Similarly, in the case of vehicles outside the communication range of an RSU, they can evaluate each other based on the direct and indirect interactions, as well as on the last historical report of the RSU. The latter will be taken more or less into account depending on its freshness. In other words, we use the report's reception time (T0) with the current time (T) to compute its importance factor $\frac{T_0}{T}$. Then, the global trust evaluation (GTR) given by a node i to another node j is updated using equation 7:

$$GTR(i,j) = (1 - \frac{T_0}{T}) \cdot \big[(\beta \cdot DTR(i,j)) + (\alpha \cdot ITR(i,j))\big] + (\frac{T_0}{T}) \cdot \big[HRSU(j)\big] \tag{7}$$

In addition, if the new global trust evaluation $GTR(i,j)$ increases compared to its previous value, a positive recommendation about the node j is automatically broadcasted. In the other hand, if $GTR(i,j)$ decreases bellow a predefined threshold a negative recommendation is broadcasted.

4.4. ETSI-based trust establishment

In the facilities layer defined in the ETSI standard, the main components are the CAM and DENM basic services.

Cooperative awareness within road traffic means that road users and the roadside infrastructure are informed about each other's position, dynamics and attributes. Cooperative Awareness Messages (CAMs) are exchanged in the ITS network between ITS-Ss (Intelligent Transportation System-Stations) to create and maintain awareness of each other, and to support cooperative performance in the road network [39]. In addition, ETSI ITS has defined a "Basic Set of Applications" where the Road Hazard Warning (RHW) application is composed of multiple use cases. Those applications are supported by the decentralized environmental notification (DENM) basic service [40].

In this work we take advantage of these messages (CAMs and DENMs) to continuously, and in a distributed manner, estimate the traffic density, the existence of dishonest nodes within road segments, and the trust-level associated to different events and their dissemination.

Involved modules in this phase are shown in figure 6

4.4.1. Segments' trust and traffic estimation

To estimate the degree of trust and the traffic density between two road junctions in a collaborative and distributed manner, we use three information sources: the total Number of Front and Rear Nodes (NFN, NRN), the rate of Trusted Front and Rear Nodes (TFN/TRN), and the Minimum Trust of Nodes in the Front and Rear (Min(TFN)/Min(TRN)).

We used the trusted nodes rate (TFN and TRN) in addition to the total number of nodes (NFN and NRN) to have a clear idea about the traffic density. Furthermore, in the message forwarding process, untrusted vehicles will be avoided because they behave as blackholes dropping messages.

The Minimum trust values (Min(TFN), Min(TRN)) are used to know the dishonest nodes distribution within the road segments.

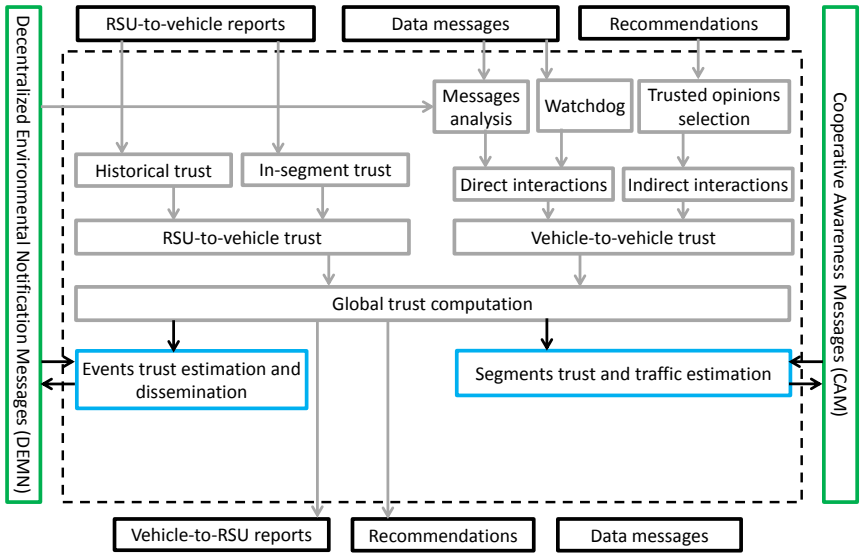

Figure 6: Events' trust, segments' trust, and traffic estimation modules.

Figure 7 represents a numerical example of such information carried by a vehicle labeled as A.

For fields Min(TFN) and Min(TRN), a value of 1 would only take place if all vehicles in a specific segment have a special role (e.g. police, ambulance), but this situation is not realistic, and so a value of 1 will never be reached (minimum trust will always be less than 1). A similar value can be achieved if all nodes within a segment consider each other trusted vehicles (*trusted vehicles ratio* = 1). In addition, every node i associates the previously computed trust value *GTR(i, j)* to each neighbor (see section 4.3).

We chose to take advantage of CAM messages [39] by adding our security-related fields. This allows us to estimate the trust, the traffic density, and the dishonest nodes distribution within a road segment. More specifically, we extend the high frequency container since information within this container is continuously updated, which is also the case for traffic density and the trust values of nodes. The new format contains the previously mentioned information: Total Number of Front and Rear nodes (NFN, NRN), the Ratio of Trusted

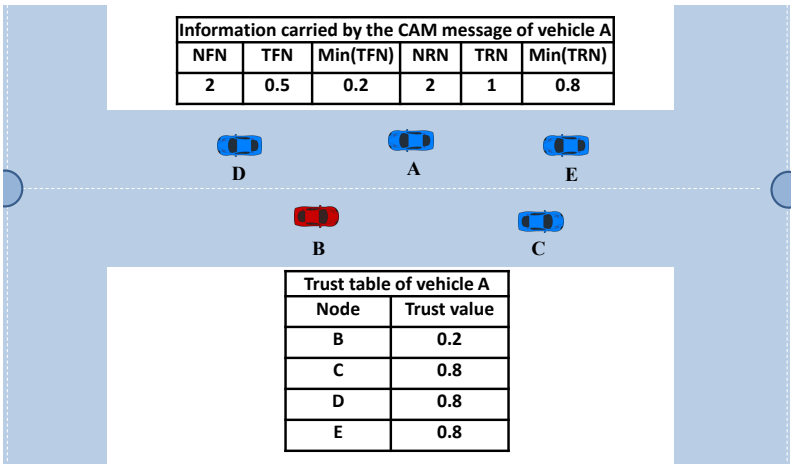

Figure 7: An example of traffic density and segment's trust information.

Front and Rear nodes (TFN/TRN), and the Minimum Trust at Front and Rear (Min(TFN)/Min(TRN)), as illustrated in figure 8.

In particular, to optimize the length of our fields, we represent the float information (TFN, TRN, Min(TFN), Min(TRN)) using only one byte. For example, if the Trusted Nodes Rate in the rear (TRN) is 0.99, carried value in TRN will be $(99)_2$.

Nodes maintain local information about their one-hop neighbors to perform trust and traffic density estimations. For the traffic estimation, the maintained fields are: (i) 'MyNFN' and 'MyNRN', which store the total number of one hop front/rear neighbors; (ii) 'MyTFN' and 'MyTRN', that store the ratio of trusted one hop front/rear neighbors; and (iii) 'Min(TFN) and 'Min(TRN)', for the minimum trust in one hop front/rear neighbors.

Upon receiving a CAM message from the front or rear sides, the vehicles compare it with their own neighborhood information. The goal of this comparison is to gather accurate and precise information about the segment, meaning that this information will be used later on by vehicles located at junctions to choose the best segment, and by in-segment vehicles to choose the most adequate next

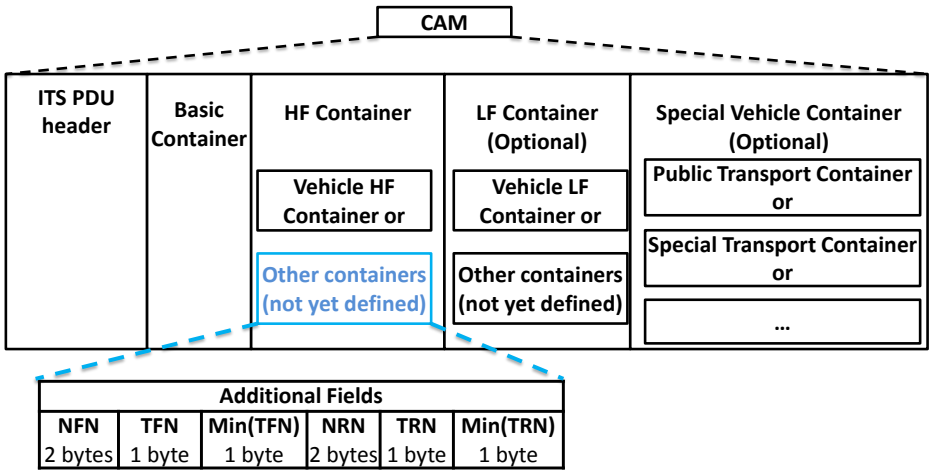

Figure 8: Additional Fields.

hop for unicast data messages.

For more accuracy, every node i only takes into account messages coming from its farthest trusted neighbor j both at front and rear to select the most accurate and fresh information, updating its current security metrics following algorithm 2.

When a vehicle 'i' located within a road segment receives a CAM message broadcasted by another node 'j' located at its front/rear, it computes: the number of front/rear vehicles, the front/rear trusted vehicles ratio, and the minimum trust value of front/rear vehicles. Since we take into account just CAMs coming from trusted nodes 'j', these last can be located near to the receiver node 'i'. Hence, to avoid re-counting common neighbors we used the 'cardinal' function.

In the other hand, if the vehicle 'i' is located within a junction, it associates a weight called SW ("Segment Weight") for every segment 'k', this weight is computed using the received traffic and trust information from vehicles located in segment 'k', and it will be used later on to choose the most adequate path in the message routing process.

Algorithm 2 Segments' trust and traffic estimation

INPUTS: CAM messages broadcasted by j and received by i.
OUTPUTS: updated CAM for i; segments' weights computed.
Upon receiving the estimation fields from j by i;
if (i is located within a road segment) **then** (see figure 2 in-segment part)
    if (j in front of i) **then**
        NFN(i) ← MyNFN + NFN(j) - [Card(one hop Front Neighbors of i ∩ Front Neighbors of j)];
        TFN(i) ← MyTFN + TFN(j) - [Card (one hop Trusted Front Neighbors of i ∩ Trusted Front Neighbors of j)];
        Min(TFN) ← Min [MyMin(TFN), Min(TFN)(j)];
    else (j in rear of i)
        NRN(i) ← MyNRN + NRN(j) - [Card(one hop Rear Neighbors of i ∩ Rear Neighbors of j)];
        TRN(i) ← MyTRN + TRN(j) - [Card (one hop Trusted Rear Neighbors of i ∩ Trusted Rear Neighbors of j)];
        Min(TRN) ← Min [MyMin(TRN), Min(TRN)(j)];
    end if
else (i is located within a junction, see figure 2 in-junction part)
    ∀ k ∈ { A, B, C}
    if (The vehicle in 'k' is entering the junction) **then**
        $SW_k \leftarrow NFN_{V_k} \cdot TFN_{V_k} \cdot Min(TFN)_{V_k}$;
    else (The vehicle in 'k' is leaving the junction)
        $SW_k \leftarrow NRN_{V_k} \cdot TRN_{V_k} \cdot Min(TRN)_{V_k}$;
    end if
end if
End

4.4.2. Event trust and trusted alert dissemination

DENM messages are mainly used by cooperative Road Hazard Warning (RHW) applications in order to alert road users about the events detected. A co-

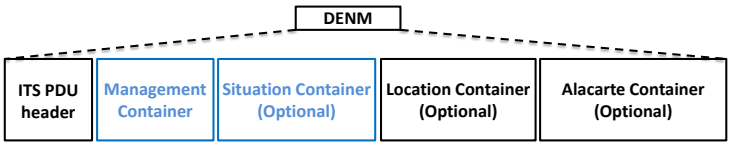

Figure 9: DENM format.

operative RHW application is an event-based application composed of five containers, where two of them are mandatory (ITS PDU header and Management Container), and the other three are optional (Situation Container, Location Container, and Alacarte container). For more details about these containers, please refer to [40].

In addition to the ITS PDU Header container, in this work we focus on the management, and the situation containers (see Figure 9).

In the Management container, some event-related information is defined including the traffic direction, the validity duration and the relevance distance representing the maximum distance beyond which DENMs should not be disseminated. This important information will be used in the dissemination part in addition to the computation of DENM similarities.

For the situation container, the application layer provides an information quality value varying from 0 to 7 representing the event's message effectiveness. A classification of events, along with a set of 99 event-related causes, are also available in the standard, which can improve the similarity evaluation [40].

Generally, the trust given to a specific event is related to the level of honesty associated to the event report originator. In addition, some context-based information may be used to ensure reliable event report dissemination. For example, we can decide not to accept notifications about ice on the road when having a temperature superior to 20, or that a road is congested from midnight to 6 a.m in normal situations. To this end, DENM messages contain fields describing the reported event in a clear and precise manner.

Operations that can be done on these messages are three: triggering, updating and termination of the event. While the first two are a task of the originator

node, the third one includes cancelation and negation, and it can be done by any intermediate node.

Unlike nodes' trust, the event's trust (ETR) is a value computed on the fly for a specific event. In our case, this value is computed using the originator global trust (GTR) and the event credibility through the received information quality (from the situation container). Then, if the event's trust is higher than a predefined threshold, a validity test is done on the DENM before rebroadcasting it; otherwise, it is dropped. In addition, if node i decides to rebroadcast node j's event messages, it increases its message quality $Qmsg(i,j)$, decreasing it otherwise since this communication is considered a direct interaction. Algorithm 3 describes the proposed trust-based DENM dissemination process:

Algorithm 3 Trust-aware DEN messages dissemination process

1: **INPUTS**: Alert of an event 'E' sent by a node j (DENM message).
2: **OUTPUTS**: Direct interaction evaluation; relay or drop the alert.
3: Upon receiving a DENM;
4: $ETR(E,j) \leftarrow \rho \cdot InfoQuality(E)+(1\text{-}\rho)\cdot GTR(i,j)$;
5: **if** $(ETR(E,j) \geq$ TrustToSend) **then**
6: $Qmsg(i,j) \leftarrow Qmsg(i,j)+\delta$;
7: **if** (Relevance distance and Validity duration) $\leq$ limits) **then**
8: Broadcast (DENM);
9: **else**
10: Cancel (DENM);
11: **end if**
12: **else**
13: $Qmsg(i,j) \leftarrow Qmsg(i,j)\text{-}\mu$;
14: **end if**
15: **End**

In the case of DENM messages, and since we focus on safety situations, we give more importance to the event information quality than to its originator's trust. This is achieved by multiplying it by the message credibility factor (ρ),

which is in the range $0.7 \leq \rho \leq 1$, thereby insuring that message credibility has always a higher impact. The event information quality ($InfoQuality(E)$) is a field included within every generated DENM representing the credibility of the reported event E; for more details please refer to [40].

In addition, we consider DENM's information as a vector A of n elements. Every element represents the value of specific information parameters. For instance: A[1] = event latitude, A[2] = event longitude, A[3] = validity duration, etc. Then, for every pair of sources *(Vj, Vk)*, we perform an offline computation of the similarities between DENMs describing the same event, but coming from different sources *Vj*. Finally, common sources in all inadequate similarities have their trust level decreased. By comparing information carried by periodical CAM messages to the RSU, the latter will be able to detect whether trusted nodes within a road segment are more or less numerous than malicious ones. Based on this information, it decreased the RSU historical trust (HRSU) of vehicles with low similarity values. Algorithm 4 summarizes this process:

Algorithm 4 Events reporters honesty using DENMs similarity

INPUTS: A set of nodes Vi reporting a same event.
OUTPUTS: Historical RSU-to-vehicle trust updated.
For every pair of event reporters *(Vj, Vk)* do;
Similarity*(Vj, Vk)* $\leftarrow \frac{1}{\sum_{i=0}^{n}(A_{Vj}[i]-A_{Vk}[i])^2}$;
if *Vj* and *Vk* reports are not similar **then**
    Increment (Counter of *Vj* low similarities);
    Increment (Counter of *Vk* low similarities);
end if
if TFN|TRN $\geq$ NFN|NRN/2 **then** (there are more trusted than dishonest nodes)
    if (*Vj* appearance frequency $\geq$ NFN|NRN/2) **then**
        HRSU(j)$\leftarrow$ *HRSU(j)*-μ;
    end if
else (there are more dishonest nodes than trusted ones)
    if (*Vj* appearance frequency $\leq$ NFN|NRN/2) **then**
        HRSU(j)$\leftarrow$ *HRSU(j)*-μ;
    end if
end if
End

A_{Vj} and A_{Vk} are the vectors representing the DENM's information of vehicles j and 'k', respectively.

5. Trusted communication and data routing

In addition to the continuous trust and traffic estimation, our additional fields carried by CAM messages allows in-junction and in-segment nodes to collaborate with each other to choose the most suitable path to the destination whenever data must be delivered (see figure 2).

Involved modules in this last phase are shown in figure 10

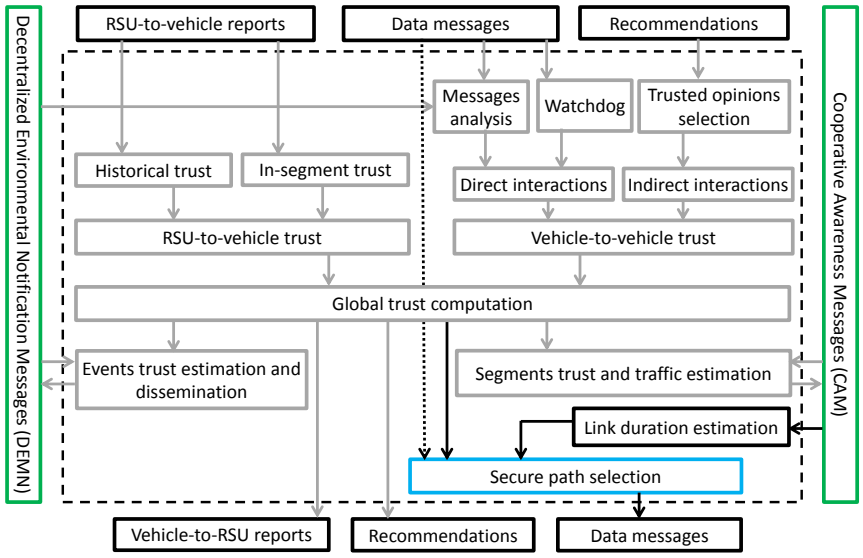

Figure 10: Trusted communication and data routing modules.

Upon receiving a data message, node i checks the source's trustfulness GTR(i, source). If it is lower than the predefined 'TrustToSend' threshold, the message will be dropped; otherwise, the forwarding process continues. Then, if vehicle i is the end destination, it performs data verification on the received message. This verification allows evaluating the senders' behavior based on the quality of its message. If node i is just an intermediate node, we distinguish two cases:

- In-segment case: if the position of i is within a segment, it has to select as the next hop the most trusted, stable and close to the destination/junction node among its neighbors.
- In-junction case: if the position of i is within a junction, it has to select the most trusted and close segment to the destination to forward the message through it.

Algorithm 5 summarizes the data delivery process:

Algorithm 5 Trust-aware inter-vehicular communication

INPUTS: Data message sent/forwarded by j to i.
OUTPUTS: Data message accepted/dropped; Direct trust updated; Best path selected .
When a data message from 'source' is received by i;
if ($GTR(i, Source) \geq$ TrustToSend) **then**
  if (End destination is i) **then**
    Data verification (msg);
    if (legal (msg)) **then**
      $Qmsg(i, Source) \leftarrow Qmsg(i, Source)+\delta$;
    else
      $Qmsg(i, Source) \leftarrow Qmsg(i, Source)$-$\mu$;
    end if
  else
    if (Destination is a neighbor of i) **then**
      Deliver ('msg' to destination);
    else (i is an intermediate node)
      if (i is an In-segment node) **then**
        For every neighbor 'k' of i
        if (Destination in segment) **then**
          Score(k) $\leftarrow \frac{GTR(i,k) \cdot LD(i,k)}{Distance(k,destination)}$;
        else (Destination out of segment)
          Score(k) $\leftarrow \frac{GTR(i,k) \cdot LD(i,k)}{Distance(k,nextjunction)}$;
        end if
        Transfer ('msg' to 'k' having max score);
      else (i is an In-junction node)
        For every segment 'k';
        Score(k) $\leftarrow \frac{SW(k)}{Distance(junction,destination)through'k'}$;
        Transfer ('msg' through 'k' having max score);
      end if
    end if
  end if
else (low trust $GTR(i, source)$)
  Drop (msg);
end if

δ, μ are the trust increment and decrement factors. We take $\delta \ll \mu$ since peer trust is difficult to build up but easy to tear down.

'SW' is the segment weight computed in the continuous trust and traffic estimation presented in the previous section. $LD(i, k)$ is an estimation of the link duration between the two nodes i and k, and it is computed as follows:

- In the case of two vehicles moving with similar directions:

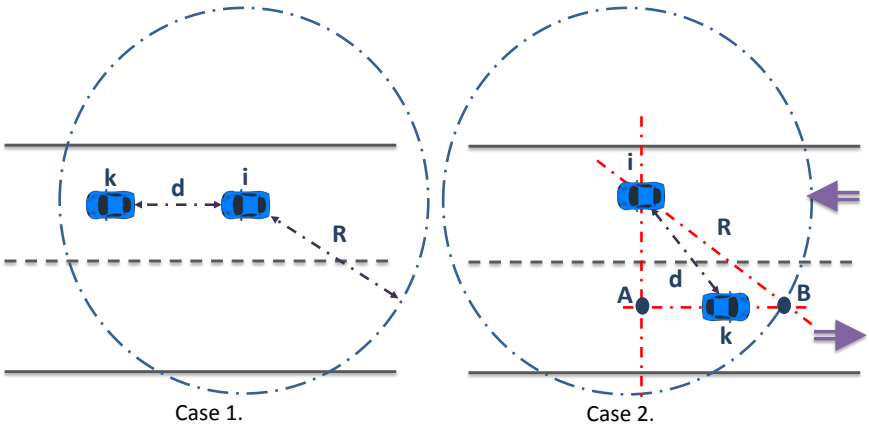

Figure 11: Link duration estimation.

$$LD(i,k) = \begin{cases} \frac{R+d}{|V(i)-V(k)|} & V(i) \geq V(k) \\ \frac{R-d}{|V(i)-V(k)|} & V(i) < V(k) \end{cases}$$

Where $V(i)$ is the velocity of i, R is the communication range, and d is the distance between i and k.

- In the case of two vehicles moving in opposite directions:

$$LD(i,k) = \frac{|L+X|}{|V(i)-V(k)|}$$

Where $L = \sqrt{R^2 - (y_i - y_k)^2}$; $X = x_i - x_k$; $L = distance(A,B)$ and $X = Distance(A,k)$ (see figure 11).

6. Performance evaluation

To evaluate our Trust establishment scheme we relied on the NS-2 simulator [41]. The generated vehicular traffic is based on the Citymob mobility model [42], which uses SUMO [43] to create mobility traces based on real maps extracted from OpenStreetMap. In our case we used a map from the downtown area of Valencia, Spain (see figure 12).

Table 2 summarizes the main simulation parameters:

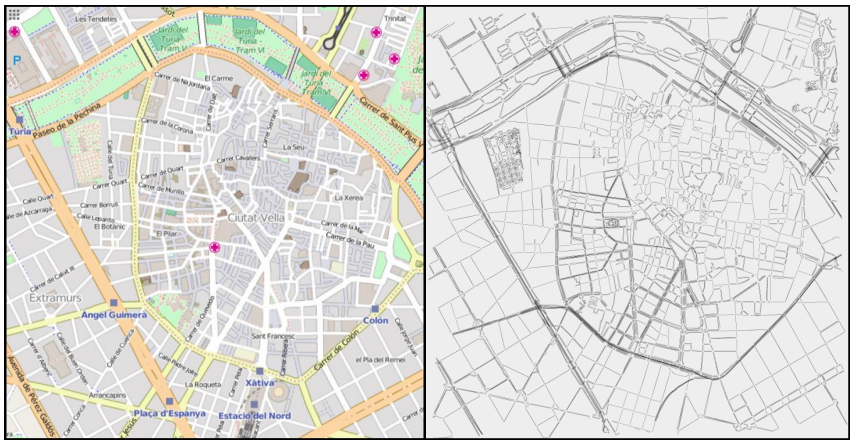

Figure 12: Simulated scenario of Valencia city, Spain.

Table 2: Simulation parameters.

Parameters	Value
Simulation area (km×km)	2×2
Transmission range(m)	300
Permissible lane speed (km/h)	[0,80]
Number of vehicles	[0,400]
State cars percentage (fully trusted) (%)	2
All trust metrics initial values	0.5
α	0.4
β	0.6
δ	0.01
μ	0.1
RL	0.2
ρ	0.7

Trust increment and decrement factors (δ, μ) are the same as in [13], while

the values of α, β, RL and ρ are chosen in such a way so as to achieve the best possible performance based on a large set of experiments.

In addition, we assume that we have 6 RSUs randomly distributed. 10 events occur at random simulation times. Moreover, vehicles can exchange unicast data messages. To avoid consuming too many resources, and considering that trust variations do not require a higher refresh rate, we have adopted a frequency of 0.5 Hz for our extended CAM messages, possibly extending only 1 message every 2 seconds with trust information, while CAM messages are transmitted at the typical 10 Hz rate.

We divide our performance evaluation section into two parts: (i) Impact on network performance when compared to an insecure routing protocol; and (ii) Security performance, describing the achieved security results when compared to other existing works.

6.1. Network performance

In this part we discuss the impact of establishing trust on the network resources in terms of: average end-to-end delay, packet delivery ratio, and network overhead. We compare our proposal against both secure and insecure versions of the GyTAR routing protocol [26, 25], in the presence of 20% of nodes acting as blackholes.

Figure 13 shows that, except for cases of very low node density, our proposal performs better than both GyTAR versions, delivering packets to their end destinations with a reduced delay, typically not exceeding a second if the number of vehicles is higher than 200.

Similarly to the Average end-to-end delay, our solution can ensure a high efficiency in terms of packet delivery ratio, approaching optimal values whenever a fully connected network is available (see figure 14)

In terms of additional overhead, figure 15 shows that our solution is injecting an acceptable load into the network, being lower than the one introduced by the GyTAR protocol. Notice that, since our solution is based on the standard, it does not add a significant amount of overhead or additional messages. This

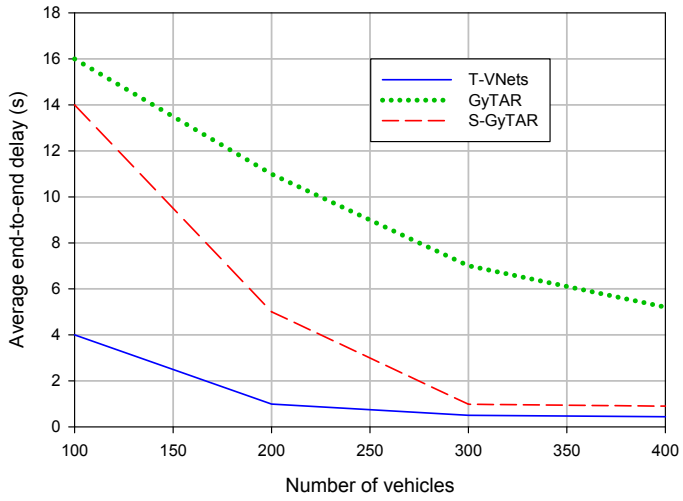

Figure 13: Average end-to-end delay of unicast data messages.

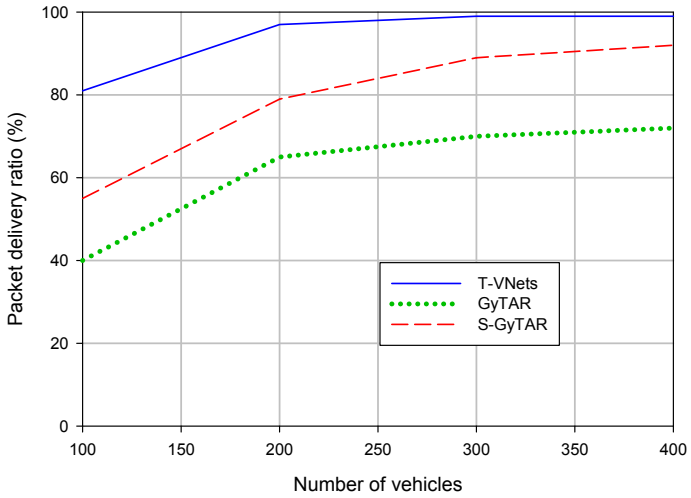

Figure 14: Packet delivery ratio.

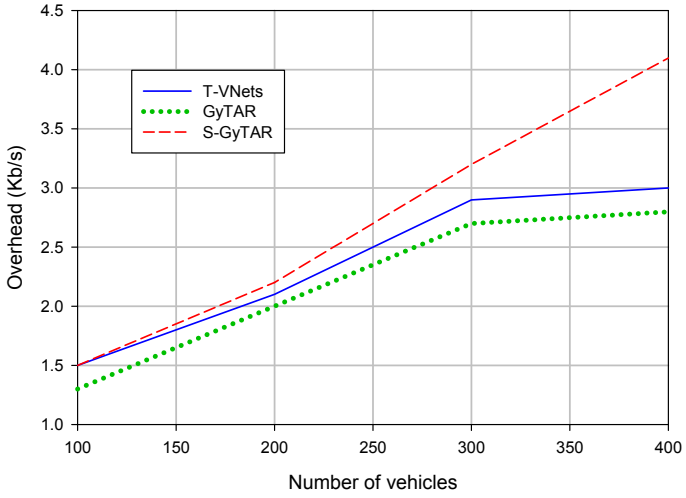

Figure 15: Generated Overhead.

means that the overhead introduced is mainly due to RSU reports and trusted nodes recommendations.

6.2. Security performance

In this part we study the achieved security results of our proposal when compared to the T-CLAIDS [14] and the AESFV [15] trust establishment schemes, in addition to the secure version of the GyTAR protocol (S-GyTAR) [25]. The comparison will be in terms of dishonest vehicles detection ratios and percentage of wrong decisions. Moreover, we analyse the impact of deactivating some elements of our security architecture on performance results.

6.2.1. Dishonest nodes detection efficiency

In this part we discuss the ability of our proposal to detect dishonest nodes compared to other existing solutions. To this purpose we fix the number of nodes within the network at 300, and configure 30% of them to behave maliciously.

Figure 16 shows that our system has detected nearly 97% of the existing dishonest nodes in about 200s, while AECFV requires 25% additional time to achieve the same results. This is due to the variety of trust metrics used, and

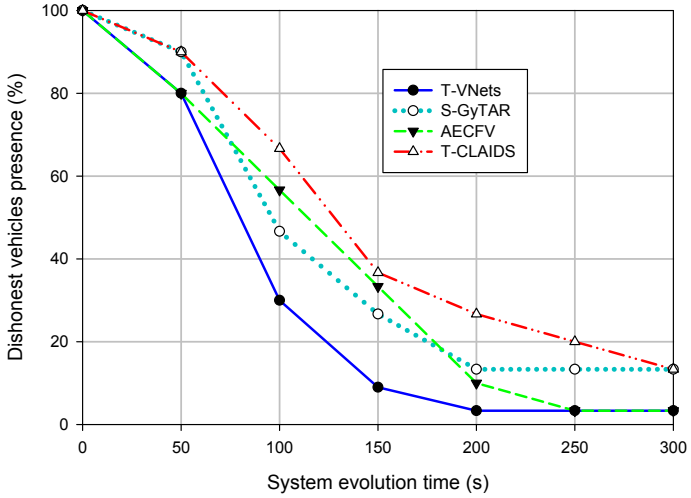

Figure 16: Dishonest nodes detection ability during 300s of simulation time.

to the ability to estimate the distribution of dishonest nodes in our system. Concerning the S-GyTAR and T-CLAIDS protocols, they achieve poorer performance levels.

In the second scenario we study the system scalability. With this purpose we vary the number of nodes within the network from 100 to 400 nodes, where 30% of them have a malicious behavior (33% keep sending messages at a high rate, 33% drop all received packets, and 33% send false alerts). In addition, dishonest nodes broadcast only positive reports about each other.

Similarly to the dishonest nodes detection results (see figure 16), T-VNets is able to maintain its resilience even in the presence of a high number of nodes, offering performance results comparable to those of the AECFV protocol, and performing much better than the two other solutions (see figure 17). This detection stability is mainly due to the cooperation among nodes, which means more information is handled to the RSUs and, therefore, more accurate decisions can be made.

The last scenario analysed measures the resilience of our proposal when varying the dishonest nodes' ratio. Figure 18 shows that our solution improves

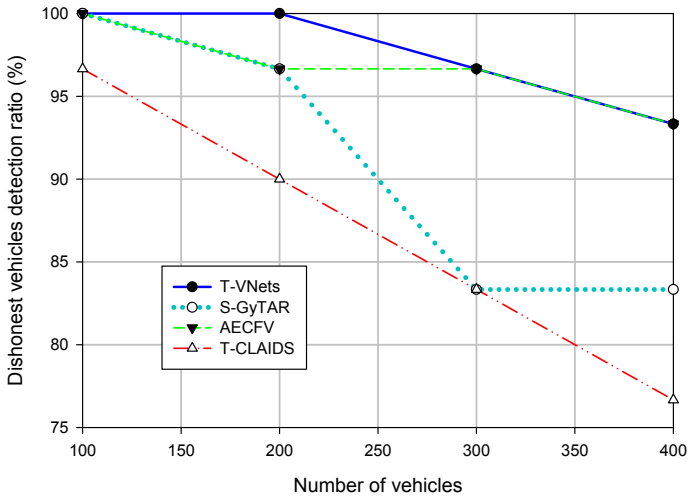

Figure 17: Dishonest nodes detection for different densities.

upon AECFV in the presence of a high ratio of dishonest nodes. This is mostly due to the fact that AECFV has no previous estimation about the ratio of dishonest nodes and their distribution within the network, contrarily to our proposal.

6.2.2. Dishonest nodes detection accuracy

Similarly to any security system for mobile and distributed networks, the existing solutions are prone to trigger some false positives when detecting dishonest nodes.

To evaluate the impact of this problem we varied the dishonest nodes ratio over a total of 300 nodes, studying how many honest nodes are wrongly considered dishonest at the end of the simulation.

Figure 19 shows that, in the detection process, T-VNets generates about 4.7% of false positives when half of the nodes are dishonest; this is generally due to their presence in a zone containing a high ratio of dishonest nodes, or because they have relayed some malicious messages coming from these dishonest nodes. This is prone to occur right at the beginning of an experiment, when no previous interactions have occurred. However, T-VNets is able to clearly

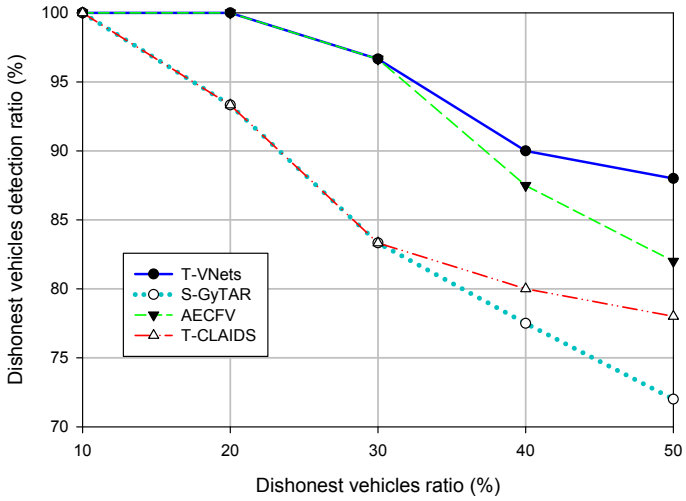

Figure 18: Dishonest nodes detection effectiveness when varying their number.

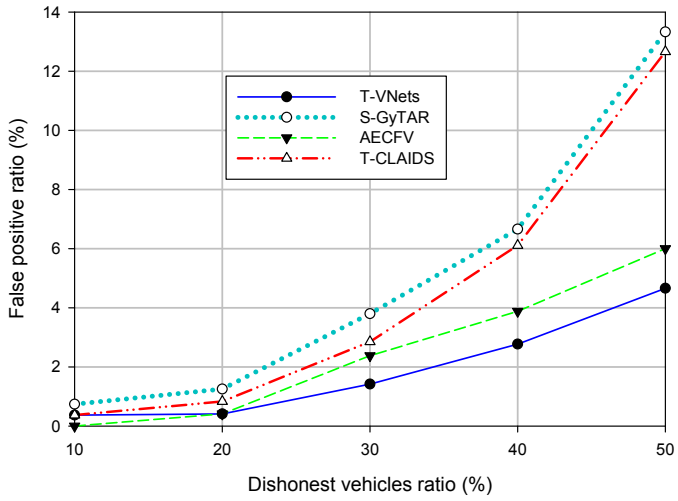

Figure 19: Generated false positive.

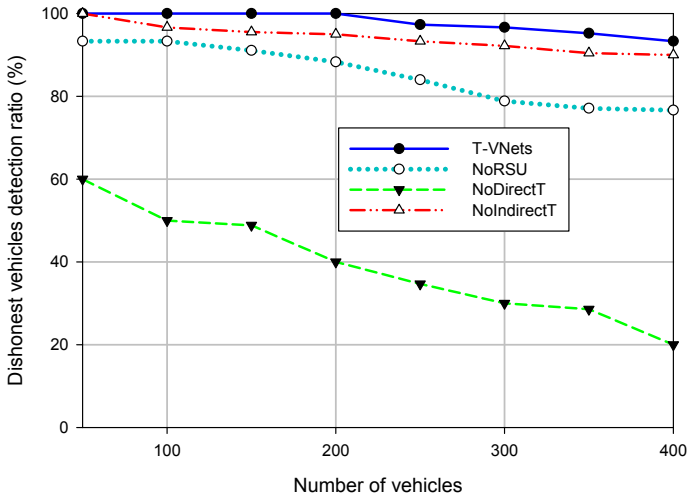

Figure 20: The different trust metrics' impacts.

provide improvements compared to the three other solutions (see figure 19).

6.2.3. Trust metrics impact

Finally, we discuss the impact of the different trust metrics used. We vary the number of node used from 50 to 400, with 30% of them behaving maliciously, and compare our protocol against other three slimmed-down versions of itself:

- *T-VNets*: this version shows the performance of our full proposal.
- *NoRSU*: it shows the performance of T-VNets when no RSUs are available.
- *NoDirectT*: it shows the performance achieved when direct trust metrics are not used. Unlike the other versions, this one is computed after 100s of simulation time since trust will never be updated if there are no interactions among nodes.
- *NoIndirectT*: it shows the performance achieved when no recommendations are exchanged among nodes.

Figure 20 shows that the key element in T-VNets is the use of direct trust metrics, which are much more relevant than the other elements (RSU and In-

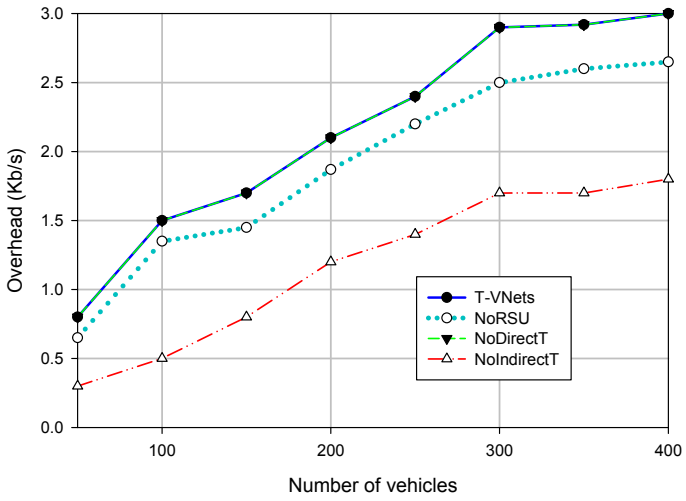

Figure 21: Generated Overhead by T-VNets different versions.

direct trust). As a result, we find that it is possible to reduce the generated overhead (see figure 21) by reducing the number of recommendations since the impact of the latter is reduced compared to the other metrics.

7. Conclusions and future work

Trust establishment in high dynamic mobile networks is a complex task due to the many challenges involved. Moreover, important standardization efforts have been made in the past years concerning VANET communications. Thus, to be readily deployable, proposed trust and security solutions should take the existing standards into account and try to take advantage of them whenever possible.

In this work we presented T-VNets, a trust establishment architecture for VANETs based on ETSI ITS standard messaging services. Our solution can offer high security levels while preserving network resources. The continuous traffic and trust estimations using CAM messages allows to quickly detect different types of active attacks, thereby avoiding untrusted paths when performing messages relaying. By evaluating event reports carried by DENM messages, our

proposal is able to enhance real-time alert dissemination processes, filtering-out non-existent or selfish alerts. In addition, our proposal accounts for direct trust, indirect trust, and RSU trust evaluations, while also considering official vehicles that offer full reliability.

Simulation results performed in realistic downtown scenarios have shown that, compared to existing works, our proposal is able to ensure high detection ratios with a low number of false positives, while preserving network resources from being exhausted.

In the future we plan to implement our proposal on mobile devices and test it in real life situations. Moreover, we plan to add other security metrics to achieve more robustness, and adapt the proposal to other international standards as well.

Acknowledgments

This work was partially supported by both the *Ministerio de Economía y Competitividad, Programa Estatal de Investigación, Desarrollo e Innovación Orientada a los Retos de la Sociedad, Proyectos I+D+I 2014*, Spain, under Grant TEC2014-52690-R, and the *Ministère de l'enseignement supérieur et de la recherche scientifique, Programme National Exceptionnel P.N.E 2015/2016*, Algeria.

References

[1] A. Vinel, L. Lan, N. Lyamin, Vehicle-to-vehicle communication in c-acc/platooning scenarios, IEEE Communications Magazine 53 (8) (2015) 192–197.

[2] M. Raya, J.-P. Hubaux, The security of vehicular ad hoc networks, in: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, ACM, 2005, pp. 11–21.

[3] I. T. S. Committee, Ieee standard for wireless access in vehicular environments-security services for applications and management messages, IEEE Vehicular Technology Society 1609.

[4] Etsi ts 102 940 v1.1.1 , intelligent transport systems (its); security; its communications security architecture and security management (2012-06).

[5] A. Zaheer, N. Venkatraman, Relational governance as an interorganizational strategy: An empirical test of the role of trust in economic exchange, Strategic management journal 16 (5) (1995) 373–392.

[6] N. Haddadou, A. Rachedi, Y. Ghamri-Doudane, Trust and exclusion in vehicular ad hoc networks: an economic incentive model based approach, in: Computing, Communications and IT Applications Conference (ComComAp), 2013, IEEE, 2013, pp. 13–18.

[7] N. Yang, A similarity based trust and reputation management framework for vanets, International Journal of Future Generation Communication and Networking 6 (2) (2013) 25–34.

[8] Q. Ding, X. Li, M. Jiang, X. Zhou, Reputation management in vehicular ad hoc networks, in: Multimedia Technology (ICMT), 2010 International Conference on, IEEE, 2010, pp. 1–5.

[9] Y. Guo, S. Schildt, L. Wolf, Using cluster analysis to detect attackers in vehicular delay tolerant networks, in: Ad Hoc Networks, Springer, 2014, pp. 181–196.

[10] T. Moore, M. Raya, J. Clulow, P. Papadimitratos, R. Anderson, J.-P. Hubaux, Fast exclusion of errant devices from vehicular networks, in: Sensor, Mesh and Ad Hoc Communications and Networks, 2008. SECON'08. 5th Annual IEEE Communications Society Conference on, IEEE, 2008, pp. 135–143.

[11] M. Raya, P. Papadimitratos, V. D. Gligor, J.-P. Hubaux, On data-centric trust establishment in ephemeral ad hoc networks, in: INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, IEEE, 2008.

[12] S. Gurung, D. Lin, A. C. Squicciarini, E. Bertino, Information-oriented trustworthiness evaluation in vehicular ad-hoc networks., in: NSS, Springer, 2013, pp. 94–108.

[13] J. Zhang, C. Chen, R. Cohen, Trust modeling for message relay control and local action decision making in vanets, Security and Communication Networks 6 (1) (2013) 1–14.

[14] N. Kumar, N. Chilamkurti, Collaborative trust aware intelligent intrusion detection in vanets, Computers & Electrical Engineering 40 (6) (2014) 1981–1996.

[15] H. Sedjelmaci, S. M. Senouci, An accurate and efficient collaborative intrusion detection framework to secure vehicular networks, Computers & Electrical Engineering 43 (2015) 33–47.

[16] J. Zhang, A survey on trust management for vanets, in: Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on, IEEE, 2011, pp. 105–112.

[17] J.-H. Cho, A. Swami, I.-R. Chen, A survey on trust management for mobile ad hoc networks, Communications Surveys & Tutorials, IEEE 13 (4) (2011) 562–583.

[18] U. Khan, S. Agrawal, S. Silakari, Detection of malicious nodes (dmn) in vehicular ad-hoc networks, Procedia Computer Science 46 (2015) 965–972.

[19] P. Golle, D. Greene, J. Staddon, Detecting and correcting malicious data in vanets, in: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, ACM, 2004, pp. 29–37.

[20] F. G. Mármol, G. M. Pérez, Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks, Journal of Network and Computer Applications 35 (3) (2012) 934–941.

[21] X. Li, J. Liu, X. Li, W. Sun, Rgte: A reputation-based global trust establishment in vanets, in: Intelligent Networking and Collaborative Systems (INCoS), 2013 5th International Conference on, IEEE, 2013, pp. 210–214.

[22] Y.-M. Chen, Y.-C. Wei, A beacon-based trust management system for enhancing user centric location privacy in vanets, Communications and Networks, Journal of 15 (2) (2013) 153–163.

[23] A. Jesudoss, S. K. Raja, A. Sulaiman, Stimulating truth-telling and cooperation among nodes in vanets through payment and punishment scheme, Ad Hoc Networks 24 (2015) 250–263.

[24] R. S. Bali, N. Kumar, Secure clustering for efficient data dissemination in vehicular cyberphysical systems, Future Generation Computer Systems (2015) –doi:http://dx.doi.org/10.1016/j.future.2015.09.004.

[25] T. Bouali, E.-H. Aglzim, S.-M. Senouci, A secure intersection-based routing protocol for data collection in urban vehicular networks, in: Global Communications Conference (GLOBECOM), 2014 IEEE, IEEE, 2014, pp. 82–87.

[26] M. Jerbi, S.-M. Senouci, T. Rasheed, Y. Ghamri-Doudane, Towards efficient geographic routing in urban vehicular networks, Vehicular Technology, IEEE Transactions on 58 (9) (2009) 5048–5059.

[27] H. Gong, L. Yu, X. Zhang, Social contribution-based routing protocol for vehicular network with selfish nodes, International Journal of Distributed Sensor Networks 2014 (2014) 700–705.

[28] H. Sedjelmaci, S. M. Senouci, M. A. Abu-Rgheff, An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks, Internet of Things Journal, IEEE 1 (6) (2014) 570–577.

[29] R. A. Shaikh, A. S. Alzahrani, Intrusion-aware trust model for vehicular ad hoc networks, Security and communication networks 7 (11) (2014) 1652–1669.

[30] A. Ltifi, A. Zouinkhi, M. S. Bouhlel, A cooperation based scheme for managing alert propagation in vanet, Wireless Personal Communications (2015) 1–21.

[31] K. C. Abdelaziz, N. Lagraa, A. Lakas, Trust model with delayed verification for message relay in vanets, in: Wireless Communications and Mobile Computing Conference (IWCMC), 2014 International, IEEE, 2014, pp. 700–705.

[32] N. Haddadou, A. Rachedi, Y. Ghamri-Doudane, A job market signaling scheme for incentive and trust management in vehicular ad hoc networks, Vehicular Technology, IEEE Transactions on 64 (8) (2015) 3657–3674.

[33] K. Rostamzadeh, H. Nicanfar, N. Torabi, S. Gopalakrishnan, V. Leung, A context-aware trust-based information dissemination framework for vehicular networks, Internet of Things Journal, IEEE 2 (2) (2015) 121–132.

[34] O. Punal, C. Pereira, A. Aguiar, J. Gross, Experimental characterization and modeling of rf jamming attacks on vanets, Vehicular Technology, IEEE Transactions on 64 (2) (2015) 524–540.

[35] N. Lyamin, A. V. Vinel, M. Jonsson, J. Loo, Real-time detection of denial-of-service attacks in ieee 802.11 p vehicular networks., IEEE Communications letters 18 (1) (2014) 110–113.

[36] O. Puñal, I. Aktas, C.-J. Schnelke, G. Abidin, K. Wehrle, J. Gross, Machine learning-based jamming detection for ieee 802.11: Design and experimental evaluation, in: World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on a, IEEE, 2014, pp. 1–10.

[37] P. Wex, J. Breuer, A. Held, T. Leinmüller, L. Delgrossi, Trust issues for vehicular ad hoc networks, in: Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE, IEEE, 2008, pp. 2800–2804.

[38] M. Gerlach, Trust for vehicular applications, in: Autonomous Decentralized Systems, 2007. ISADS'07. Eighth International Symposium on, IEEE, 2007, pp. 295–304.

[39] Etsi en 302 637-2 - v1.3.2, vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service (2014-11).

[40] Etsi en 302 637-3 - v1.2.2, vehicular communications; basic set of applications; part 3: Specifications of decentralized environmental notification basic service (2014-11).

[41] T. Issariyakul, E. Hossain, Introduction to network simulator NS2, Springer Science & Business Media, 2011.

[42] F. J. Martinez, J.-C. Cano, C. T. Calafate, P. Manzoni, Citymob: a mobility model pattern generator for vanets, in: Communications Workshops, 2008. ICC Workshops' 08. IEEE International Conference on, IEEE, 2008, pp. 370–374.

[43] M. Behrisch, L. Bieker, J. Erdmann, D. Krajzewicz, Sumo–simulation of urban mobility, in: The Third International Conference on Advances in System Simulation (SIMUL 2011), Barcelona, Spain, 2011.