Document downloaded from:

http://hdl.handle.net/10251/78525

This paper must be cited as:

Kerrache, CA.; Tavares De Araujo Cesariny Calafate, CM.; Lagraa, N.; Cano Escribá, JC.; Manzoni, P. (2016). RITA: RIsk-aware Trust-based Architecture for collaborative multi-hop vehicular communications. Security and Communication Networks. 9(17):4428-4442. doi:10.1002/sec.1618.

The final publication is available at

http://dx.doi.org/10.1002/sec.1618

Copyright Wiley

Additional Information

This is the pre-peer reviewed version of the following article: Kerrache, C. A., Calafate, C. T., Lagraa, N., Cano, J. C., & Manzoni, P. (2016). RITA: RIskaware Trustbased Architecture for collaborative multihop vehicular communications. Security and Communication Networks, 9(17), 4428-4442, which has been published in final form at http://onlinelibrary.wiley.com/doi/10.1002/sec.1618/abstract

RITA: RIsk-aware Trust-based Architecture for collaborative multi-hop vehicular communications

Chaker Abdelaziz Kerrache[a,*], Carlos T. Calafate[b], Nasreddine Lagraa[a], 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

Trust establishment over vehicular networks can enhance the security against probable insider attackers. Regrettably, existing solutions assume that the attackers have always a dishonest behavior that remains stable over time. This assumption may be misleading, as the attacker can behave intelligently to avoid being detected. In this paper we propose a novel solution that combines trust establishment and a risk estimation concerning behaviour changes. Our proposal, called *RITA*, evaluates the trust among vehicles for independent time periods, while the risk estimation computes the behavior variation between smaller, consecutive time periods in order to prevent risks like an intelligent attacker attempting to bypass the security measures deployed. In addition, our proposal works over a collaborative multi-hop broadcast communication technique for both Vehicle-To-Vehicle (V2V) and Vehicle-To-Roadside unit (V2R) messages in order to ensure an efficient dissemination of both safety and infotainment messages. Simulation results evidence the high efficiency of *RITA* at enhancing the detection ratios by more than 7% compared to existing solutions, such as T-CLAIDS and AECFV, even in the presence of high ratios of attackers, while

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

offering short end-to-end delays and low packet loss ratios.

Keywords:
Trust Management, Vehicular Ad-hoc Networks, Risk estimation, Message dissemination.

1. Introduction

Securing communications in distributed and collaborative networks is always a challenging task, and it is even becoming mandatory in most cases. Usually it requires adopting case-specific and situation-adaptable communication protocols addressing the different security issues. In wireless environments, achieving an adequate security level is more challenging than in wired environments due to the open communication medium. In addition, the assumption that all peers are honest, trustful, and collaborative is not always true.

Many efficient security solutions have been proposed to secure wireless and collaborative communications, most of them being based on a centralized administration or a trusted third party. However, in mobile distributed networks, security remains an open and complex problem, especially in the case of infrastructure-less networks, usually called Mobile Adhoc NETworks (MANETs), where there is neither a centralized administration nor a stable topology.

A subcategory of MANETs that inherits all the aforementioned problems are Vehicular Adhoc Networks (VANETs). Having as its main aim the enhancement of road safety, most of its applications are based on distributed and collaborative communications among vehicles (vehicle-to-vehicle communication) and between vehicles and roadside units (vehicle-to-infrastructure communication). In this scenario, RoadSide Units (RSUs) are assumed to be the link between vehicles and such trusted third party, or be the trusted third party itself.

Similarly to MANETs, VANETs can use existing cryptography-based solutions to overcome the different kinds of external attacks [1]. However, in addition to the cryptography cost in terms of overhead and processing time, these solutions cannot punish nor detect those attacks launched by an authorized vehicle

(inside attacker). For this reason, researchers have proposed novel trust management solutions inspired by economic science to deal with such unexpected inside attackers [2]. Unlike cryptography-based solutions, trust management has lower computational requirements and introduces a lower overhead, while also supporting mobility; however, it cannot detect outsider attackers. Hence, trust modeling can be seen as an additional security technique that fills the gap of cryptography-based solutions. Moreover, trust is widely adopted as a replacement for cryptography, especially for delay-sensitive applications like VANET safety and real-time multimedia streaming applications.

Establishing trust in VANETs is based on the common assumption that trust must be hard to obtain and easy to lose, which means that network entities must strive to increase the level of trust on themselves through their honesty and an adequate network collaboration, while such trust can be lost through a relatively lower number of dishonest acts [3].

In this paper we focus mainly on the problem where vehicles can become effective at achieving network disruption by alternating between legal behavior patterns and malicious attacks (*"anti-trust management"* strategies). Figure 1 illustrates this time-varying behaviour, which is similar to the On-Off attack in wireless sensors networks (WSN) [4] and known as betrayal attack in VANETs [5]. While trust management is generally based on an evaluation of historical interactions, detecting these short-term attacks is a complex task. In addition, the *bad mouthing attack* [6], which can be also seen as an anti-trust management strategy, occurs when no precautions are taken against selfish vehicles generating only bad reports about other vehicles.

Thus, we introduce an estimation of risk associated to behaviour changes as an additional process to improve trust management among vehicles, thereby attempting to avoid sophisticated attacks. Our solution aims at filling-in the gap of classical trust models when facing the aforementioned illegal behavior. Trust and risk estimation processes rely on a timing-based technique to give more importance to actions occurring in recent time instants instead of accounting for the whole historical behavior. In our case, risk estimation involves three crite-

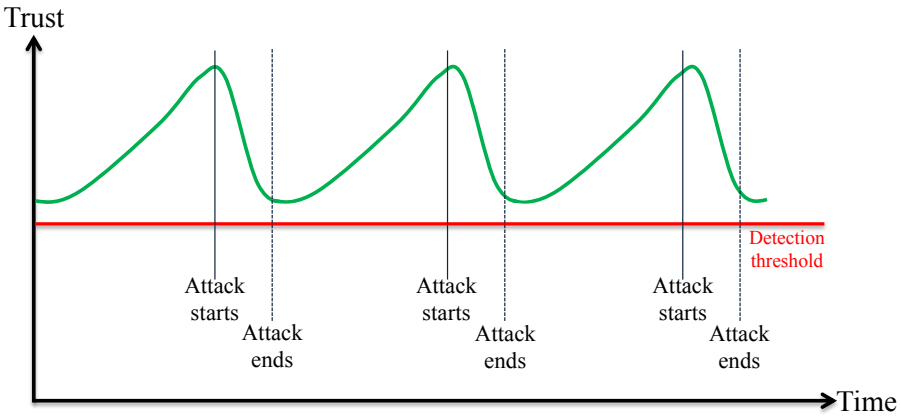

Figure 1: Intelligent dishonest behavior.

ria, which are: (i) trust variability for different time intervals, i.e., the difference between consecutive trust evaluations; (ii) safety-related behavior referring to the reported event effectiveness, since this is a main concern for vehicular networks, while also representing the in-network collaboration of vehicles; and (iii) evaluation of recommendations' quality, in order to avoid the bad mouthing attack.

Moreover, we use our trust establishment architecture to propose a novel multi-hop broadcasting technique that ensures high message delivery ratios even in the presence of vehicles acting as blackholes [7] without causing the broadcast storm problem. The adversarial model addressed in this paper focuses mainly on the betrayal, blackhole, and bad mouthing attack techniques.

The paper is organized as follows: in the next section we present an adversary-based classification of the existing trust models for VANETs. Then, an overview of our proposal called *RITA* is provided in section 3. In section 4 we clarify the trust and risk computation details. Afterward, in section 5, we explain how the trust establishment can enhance multi-hop broadcast message dissemination in VANETs. Section 6 is dedicated to the simulation parameters and results' discussion. Finally, section 7 provides some concluding remarks and the future directions for our work.

2. Related works

Existing solutions are usually classified into entity-based [8, 9, 10], data-based [11, 12], and hybrid trust models, depending on the revocation target, which can be dishonest entities, malicious messages, or both of them [13, 14, 15]. In addition, most VANET applications are based on multi-hop broadcast vehicle-to-vehicle communication, and most of the existing trust models focus on routing, path disruption, and resource exhausting attacks including blackholes and bogus messages' injection. In the following, we survey and classify the main existing works depending on their adversary models.

2.1. Trust-based solutions against replayed, altered, and injected messages

This kind of attacks can cause huge damage, especially in safety-related contexts. Hence, most of the existing works fall under this category.

The *entity-oriented trust models* presented in [8, 9] try to revoke nodes by sending falsified messages and fake information, respectively, using different techniques. Haddadou et al. [8] chose to associate a credit value to each neighbor vehicle. This credit will increase or decrease depending on the concerned neighbor's messages trustiness. Concerning Yang's solution [9], it uses the Euclidean distance to compute the similarity between nodes in terms of reported events. Unfortunately, the first solution does not differentiate between direct and indirect trust, while for the second it faces a huge problem in the case of false recommendations.

The detection of attacks related to message quality is a process that is usually based on messages themselves, which explains why some of the existing works within this category are *Data-oriented trust models* [16, 12].

Golle et al.[16] have adapted a signature-based technique in which every received message is compared to a typical model of legal VANET messages. The problem with this solution is that it is not feasible to actually build such global model; in addition, all new legal messages will be dropped as well. Unlike [16], Gurung et al. [12] use three main metrics to classify received messages into

either legal or malicious messages; these metrics are content similarity, content conflict, and routing path similarity. However, in addition to its high time complexity, this solution does not take into account the high level of mobility associated to VANETs, nor the case of node sparsity.

Some *Hybrid trust models* have been also proposed in this same context including [13, 17]. Zhang et al. [13] propose a semi-distributed trust framework for message propagation and evaluation; in their approach the clusterheads are responsible for broadcasting and then gathering opinions about the broadcasted messages. Afterward, they decide either to drop untrustworthy messages or relay legal messages with the aggregated opinions to the next cluster in order to continue the dissemination process. Similarly to other cluster-based techniques, the clusterhead election and the probability of malicious nodes becoming clusterheads are the main problems of this solution.

Differently from the aforementioned works, Marmol et al. [17] prefer associating a confidence value to exchanged messages in addition to the gathered recommendations from both RSU and nearby vehicles to build three fuzzy sets (no trust, +/-trust, trust). The message will be dropped if it belongs to the first set, accepted but not forwarded for the second set's case, and both accepted and forwarded for the trusted messages set. The number of recommendations and their trustworthiness remain as the pending problems of this solution.

2.2. Trust-based solutions against blackholes

Inter-vehicular communication is the enabling process supporting ITS over VANETs. Hence, forcing nodes to be collaborative is an indispensable task. Solutions falling under this category try to detect selfish nodes acting as blackholes in order to ensure a more efficient forwarding process for both safety and data messages.

The *Entity-oriented trust model* proposed by Khan et al. [18] proposes computing a distrust level for every neighbor acting as a blackhole through a watchdog technique. This distrust level will be sent to the clusterhead, and in turn delivered to a third trusted party that revokes the attacker certificate. Unfor-

tunately, authors did not detail the different communication steps involved, nor the overhead associated to the cluster-based implementation. Whereas, in our previous work called $TROUVE$ [19], the idea was taking advantage of existing CAM messages, which are periodically exchanged according to the ETSI-ITS European standard [20], in order to estimate the distribution of the selfish nodes within the network and, hence, select the most trusted path avoiding these blackholes. However, this solution only addresses unicast data traffic in urban environments.

To deal with blackholes and the selective forwarding (greyholes) procedure, some *Hybrid trust models* are also available [15, 21]. The first solution, proposed by Sedjelmaci et al., is a two-level intrusion detection system, the first one being based on a collaborative in-cluster detection, and the second one on a global detection processed by the RSU. The main weaknesses of this solution are the excessive time associated to clusterhead election, and the assumption concerning stable clusters around fixed RSUs.

The work of Haddadou et al. [21], called DTM^2, proposes forcing nodes to be cooperative by establishing a communication cost. The latter is higher for selfish nodes, decreasing alongside with in-network collaborativity. How to choose the initial cost, and how to differentiate between selfish behavior and packet loss due propagation issues are the mains questionable points of this work.

2.3. Trust-based solutions against jamming and denial of service (DoS) attacks

Similarly to blackholes, jamming and DoS attacks can also prevent important information to be delivered on time, thereby disturbing VANET functionality.

Raya et al. [11] propose a *Data-oriented trust model* for Ad-hoc ephemeral networks. This model uses different trust metrics, in addition to the *a priory* fixed entities trust (e.g. $Trust(Police\ vehicles = 1;\ ordinary\ vehicles = 0.5)$), in order to detect whether the reported events are real, or if it is just an attempt to jam bandwidth. They also propose evaluating the evidences related to the reported events using Dempster-Shafer theory and Bayesian inference. The

problems of this solution are the fixed entities trust and the required training phase, which cannot be ensured in practice.

In a previous work [22], we proposed to enhance the message relaying procedure to detect DoS attacks in a fast manner through the use of an intrusion detection module. The latter takes advantage of the access categories of 802.11p in the context of dedicated to short-range communications (DSRC) in order to classify the received messages at an early stage and, hence, accelerate the intrusion detection process. Same as all existing solutions, this approach assumes that the adversary has a malicious behaviour that remains stable throughout time, thus not being a valid solution under nodes acting with an intelligent dishonest behaviour.

2.4. Trust-based solutions against fake location and timing attack

The *Data-oriented trust model* proposed by Shaikh et al. [23] is an intrusion-aware trust model that differs from other works by being capable of detecting fake location and timing values generated either by the event's reporter or the message forwarder. In this event-related solution, authors propose the computation of a confidence value for each message coming from a unique source. In addition, for all messages describing a same event, a trust value is calculated using the previously computed confidence information. Finally, accepting or rejecting an event message depends 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.

2.5. Unspecified adversarial model

In addition to the aforementioned trust models, in some works authors do not specify an adversarial model, nor the types of attack they support. Instead, they only address trust establishment over the inter-vehicular communication link.

The only *Entity-oriented trust model* falling under this category was proposed by Jesudoss et al. [24]. In particular, authors propose a clustering technique to reduce the communication overhead and assign a reputation weight to

all nodes participating in the clusterhead election and network control tasks by sharing their reports about exchanged traffic. Unfortunately, this scheme does not respect reference trust metrics such as direct and indirect trust. Moreover, high mobility levels can cause this scheme's performance to decrease considerably.

Works in [14, 25, 26, 27] are examples of *Hybrid trust approaches*.

Li et al. [25] propose a reputation-based trust establishment scheme for VANETs where the messages and their senders are evaluated based on the direct trust, indirect trust and node reputations. The main drawback of this scheme is its centralized trust computing procedure through the use of an additional infrastructure Called RMC (Reputation Management Center).

Under the assumption that all application messages are encrypted, Chen et al. [26] propose a beacon-based trust model for enhancing users' location privacy in VANETs. The proposed system can secure the VANET while maintaining privacy by using two kinds of messages: beacons and event-based messages. The main idea is crosschecking the plausibility of these two types of messages to decide if other messages are trusted or not. Despite preserving the privacy of far-away vehicles (at more than one hop), this scheme cannot efficiently evaluate all kinds of messages, nor can it detect attacks occurring at upper layers (routing, application, etc.). In addition, whenever an obstacle appears between two neighboring vehicles, this scheme causes those two vehicles to judge each other as liar and malicious.

T-CLAIDS [14] is another work providing a trust-aware intrusion detection solution for VANETs. This solution takes into account the number of vehicles, their mobility, and their motion direction to perform an action. It also maintains a probability matrix of all actions which is updated in the iterations that follow until convergence to a particular value is achieved. This way, it offers an approximate representation of a global knowledge about the environment. Unfortunately, even if this solution shows good results in the general case where malicious behaviors are stable throughout time, it looks questionable in the case of unpredictable events or attacks. 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.

Last but not least, Rostamzadeh et al. [27] try to divide the map into different areas, and the traffic into three categories: safety, infotainment, and third party services, such as inter-transportation vehicular communication. In this solution, called "FACT", the message source should be known by piggybacking the identities of all vehicles participating in the routing process. Meanwhile, an admission module is responsible for analyzing the messages using the traffic category and the piggybacked identities' trust. If the degree of satisfaction is high, a trusted path is selected for the message. Unfortunately, this solution adds a considerable overhead and processing delay. Moreover, authors do not provide information about its security performance.

2.6. State of the art review considerations

Through this hovering upon the existing solutions in the literature, it becomes clear that the adversarial models adopted assumes a consistent dishonest behaviour throughout time. In addition, none of the existing works has studied the case of specific attacks against trust models themselves.

In addition, the assumption of many works about creating a global knowledge of the network [16, 11, 25, 14] can be effective in MANETs or similar environments that are less dynamic than VANETs. Moreover, relying on RSU deployment for trust establishment [19, 15, 25] can also become a handicap since (i) they are not always present, and (ii) the trust relationship is mostly related to direct peer-to-peer interactions rather than peer-to-authority interactions.

Furthermore, many trust-based security solutions for VANETs [17, 8, 9, 23, 19] focus on improving the unicast and routing data exchange. However, critical VANET applications such as safety and service discovery are based on broadcast and multi-hop communication instead.

In this work, we propose a trust establishment technique for collaborative multi-hop communications called *RITA*. We enhance the trust computation by relying on risk estimation to deal with *"anti-trust management"* attacks. Hence,

our proposal can deal with both regular and intelligent attacks against classical trust-based solutions.

3. RITA Overview

The overall architecture of our proposal, called RIsk-aware Trust-based Architecture for collaborative multi-hop vehicular communications ($RITA$), is illustrated in Figure 2. $RITA$ can be divided into different modules responsible for: (a) computing inter-vehicular trust, (b) estimating risk, and (c) selecting the most adequate next forwarder/broadcaster vehicles for multi-hop messages. In addition, a database that stores the different recommendations and trust variations is used to enhance trust and risk computation.

The architecture of $RITA$ takes advantage of the information carried by beacon, safety, and data messages to evaluate interactions among vehicles, which can be either direct or indirect interactions. Based on these interactions among nodes, the direct and indirect trusts are first computed and then combined to form an inter-vehicular trust evaluation (a). Simultaneously, the risk of a probably launched intelligent attack -i.e., periods with normal behaviour combined with periods with dishonest behaviour- is estimated using the variation of the local knowledge-based and recommendations-based evaluation of the messages' sources (b). A trade-off between the inter-vehicular trust and the risk estimation is then computed. This final value called 'Global trust evaluation' can help in detecting both classical and intelligent attacks. Moreover, we use the trust evaluation in next forwarder/broadcaster selection procedure (c). Hence, the per-hop broadcasters are selected among the most trusted vehicles ensuring short delays and high delivery ratios.

Furthermore, it is clear that, for direct interactions, all messages (even those initially encrypted) can be decrypted and analyzed by the end destination. Hence, a decision about whether the interaction is legal (L) or malicious (M) can be made using an interaction evaluation module.

Instead of updating trust values after each interaction, we propose defining

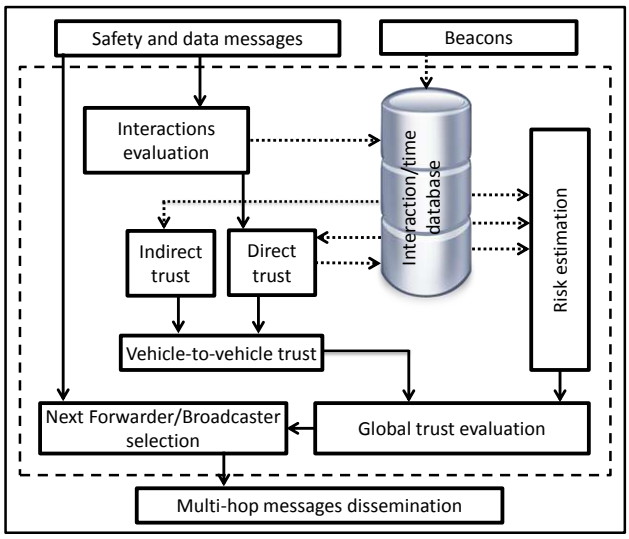

Figure 2: Proposed risk-aware modular trust establishment architecture ensuring reliable message dissemination.

small time intervals and evaluating nodes' trust on each time interval to allow quickly detecting any change in the behavior pattern. Notice that adopting long observation periods is prone to include outdated information, which has a negative impact on the trust information accuracy. Thus, we propose considering only those interactions among vehicles taking place in the most recent period T. In addition, we proposed to divide this period (T) into n time slots of the same duration, updating the trust among vehicles for every time slot t_x, where '$1 \leq x \leq n$ '. On each new time slot we discard the oldest slot assessments - similarly to a 'First In First Out (FIFO)' mechanism -, thus creating a sliding window [28]. The actual size of this window and its time slots will be based on different experimental values that will be discussed in section 6. Hence, if a node behaves legally for a long time and then starts an attack, the behaviour observed during the last slot t_x weights more than the behaviour observed in previous slots, in addition to the trust variation during these previous slots. The global trust evaluation denoted as GT, assigned by a vehicle i to another

vehicle j, combines both inter-vehicular trust $Trust(i,j)$ and the risk estimation $Risk(i,j)$, as defined in equation 1.

$$GT(i,j) = \alpha \cdot Trust(i,j) + (1-\alpha) \cdot (1 - Risk(i,j)) \quad (1)$$

In this equation α is a tuning factor used to adjust the trade-off between the inter-vehicles trust computation and the risk estimation when computing the global trust value. Notice that, since the risk estimation presents a greater error margin compared to trust estimations, it is better to choose $\alpha \geq 0.5$ to give more weight to the latter parameter; the global trust evaluation will be anyway enhanced due to the introduction of the risk estimation factor. In section 6 we assign different values to the α parameter in order to choose the most adequate value for our experiments. However, it is worth mentioning that this value should be adapted to the different situations and traffic scenarios to maximize performance. The details about how the inter-vehicular trust and risk are computed is provided in the following section.

4. RITA details: Trust and risk estimation

In this section we provide formal details about both trust and risk estimation. Section 4.1 clarifies how vehicles can compute a trust evaluation about each other based on both local knowledge-based and recommendation-based information. Then, section 4.2 is dedicated to risk computation based on behaviour changing estimations, the honesty of broadcasted recommendations, and the reported events validity.

4.1. Vehicle-to-vehicle trust computation

When focusing on inter-vehicular trust we generally distinguish between two metrics: direct trust and indirect trust. Direct trust can be defined as the local knowledge-based evaluation of the direct interactions among vehicles, while indirect trust is the evaluation of the direct interactions between two vehicles based on the opinions of other vehicles about the honesty of the two participant

vehicles. Since direct trust is more relevant than indirect (recommendation-based) trust when the number of interactions ($\#int$) increases, our vehicle-to-vehicle trust levels are adapted using the following relevance factor: $\frac{1}{\#int+1}$; this way, if we have more interactions, we assign more weight to direct trust than to indirect trust, and vice versa. Equation 2 describes how trust among vehicles is computed:

$$Trust(i,j) = \Big[\Big(1 - \frac{1}{\#int+1}\Big) \cdot DT(i,j)\Big] + \Big[\frac{1}{\#int+1} \cdot IT(i,j)\Big] \tag{2}$$

$DT(i,j)$ and $IT(i,j)$ refer to the direct and indirect trust evaluation, respectively, calculated by a vehicle i concerning another vehicle j. The computation details of $DT(i,j)$ and $IT(i,j)$ are provided in the following sections.

4.1.1. Direct trust computation

Before computing the direct trust evaluation, we denote by $H^{t_x}_{(i,j)}$ the honesty report generated by vehicle i about vehicle j using the number of legal (L) and malicious (M) interactions during a period of time t_x, where $1 \leq x \leq n$. $H^{t_x}_{(i,j)}$ is computed following equation 3:

$$H^{t_x}_{(i,j)} = \frac{L^{t_x}_{(i,j)}}{M^{t_x}_{(i,j)} + L^{t_x}_{(i,j)}} \cdot \Big[1 - \frac{1}{L^{t_x}_{(i,j)} + 1}\Big] \tag{3}$$

where $L^{t_x}_{(i,j)}$ and $M^{t_x}_{(i,j)}$ represent the number of legal and malicious interactions, respectively, between i and j from the perspective of node i. $\frac{L^{t_x}_{(i,j)}}{M^{t_x}_{(i,j)}+L^{t_x}_{(i,j)}}$ represents the percentage of legal interactions compared to the total number of interactions, and $1 - \frac{1}{L^{t_x}_{(i,j)}+1}$ is a factor that approaches 1 as the number of legal interactions increases. Hence, many legal interactions are required for a vehicle to increase its honesty index.

The direct trust computation uses the different honesty values along a period of time T by giving more importance to the last short period 't_n'. This behaviour allows $RITA$ to quickly detect misbehavior in neighboring vehicles. Equation 4

Figure 3: Proposed beacon format extension.

shows how the direct trust is updated:

$$DT(i,j) = \frac{\beta \cdot \left[\frac{\sum_{x=1}^{n-1} H_{(i,j)}^{t_x}}{n-1}\right] + H_{(i,j)}^{t_n}}{\beta + 1} \tag{4}$$

Factor β, whose value ranges between 0 and 1, is a reduction factor used to give more weight to the recent behavior of vehicles, while also taking into account their past behavior. In addition, this process is executed only for periods of time where there is at least one interaction between i and j; otherwise, the value of $DT(i,j)$ will remain unchanged.

4.1.2. Indirect trust computation

Indirect trust is calculated based on recommendations coming from one-hop neighbors about other vehicles. Most of the existing solutions suggest creating a new message type called *recommendation*, and they choose either a cluster-based technique or an aggregation method to reduce the additional overhead involved. To avoid affecting the communications bandwidth, we propose modifying the format of the periodically exchanged beacon messages by adding only two fields: (i) the neighbor identity, encoded in 1 byte, and (ii) the opinion of the beacon sender about that neighbor, also encoded in 1 byte. For example: if a node i considers that a vehicle j is untrusted, it will put the vehicle j's identity within the next beacon along with an opinion which can be < 0.5 (untrusted node) or ≥ 0.5 (trusted node). This opinion correspond to the global trust evaluation of the recommender about the recommended node $GT(i,j)$. This procedure is repeated until the entire neighbor list is included. Figure 3 illustrates the new beacon format.

Upon receiving neighbor beacons, a vehicle i computes, for every neighbor j, an indirect trust value $IT_{(i,j)}^{t_x}$ in a period of time t_x by combining the positive

and negative opinions coming from other neighbors throughout that time period.

To avoid the negative influence of dishonest vehicles' opinions, a vehicle i computes the trade-off between the different recommenders' trust and their opinions. Hence, the higher is the level of trust on a neighbor, the more is its opinion taken into account. Equation 5 shows how the indirect trust is computed by a vehicle i about another vehicle j during a period t_x.

$$IT_{(i,j)}^{t_x} = \Big[\prod_{N}\Big(DT(i,k)\cdot Opinion(k,j)\Big)^{\frac{1}{2}}\Big]^{\frac{1}{N}} \ during\ t_x, \forall k \in \{trusted\ direct\ neighbors\ of\ i\} \tag{5}$$

In this equation N refers to the number of recommenders, $IT_{(i,j)}^{t_x}$ is a combination of the recommenders' (k) direct trust DT and their opinions about the vehicle j during a period t_x. In addition, we consider a neighbor vehicle as a trusted vehicle if its global trust $GT_{(i,j)}$ is higher than a predefined threshold; this threshold can be adapted depending on the security requirements and the traffic type.

Similarly to direct trust, we assign a higher weight to the latest recommendations without forgetting the overall recommendations received. This is achieved through equation 6:

$$IT(i,j) = \frac{\beta \cdot \Big[\frac{\sum_{x=1}^{n-1} IT_{(i,j)}^{t_x}}{n-1}\Big] + IT_{(i,j)}^{t_n}}{\beta + 1} \tag{6}$$

Notice that β is the same factor used in equation 4. It is clear that, if node i does not have any direct neighbor, or if it has only malicious neighbors, the indirect trust (IT) will remain unchanged.

4.2. Risk estimation

As mentioned in the related works section, trust establishment in highly dynamic networks suffers mainly from instant behavior changes since trust is based on the accumulative historical interactions. Thus, it is hard to quickly detect changing behaviors, especially if the attackers are aware of the shortcomings

associated to trust-aware mechanisms, and make an effort to achieve high reputation values prior to launching their attack. In this context, risk estimation can be an effective solution to solve the aforementioned problem. Our $RITA$ approach allows every vehicle i to estimate a risk value for a neighboring vehicle j by combining three different factors: (i) direct trust variability (DTV) along consecutive time slots in order to detect the betrayal behavior; (ii) event-related reports (ER) represented by the ratio of fake event reports to the total number of events reports in order to punish nodes sending reports about non-existent events; and finally (iii) evaluations of recommendations (RC) to detect bad mouthing attacks, which also relies on the ratio of negative recommendations to the total number of recommendations. Equation 7 clarifies how the risk among vehicles is estimated:

$$Risk(i,j) = \frac{DTV(i,j)^2 + ER(i,j)^2 + RC(i,j)^2}{DTV(i,j) + ER(i,j) + RC(i,j)} \tag{7}$$

In this equation $DTV_{(i,j)}$ represents the maximum negative variation in direct trust given by a vehicle i to another vehicle j along different time slots, and it is calculated as follows (equation 8):

$$DTV(i,j) = \mid Min(DT^{t_x}_{(i,j)} - DT^{t_{x+1}}_{(i,j)}) \mid \forall x \in \{1, ..., n-1\} \tag{8}$$

A negative variation means that $DT^{t_{x+1}}_{(i,j)}$ is lower than $DT^{t_x}_{(i,j)}$. Hence, $DT^{t_x}_{(i,j)} - DT^{t_{x+1}}_{(i,j)}$ is a negative value and, as a consequence, the maximum direct trust variation is the absolute value of $Min(DT^{t_x}_{(i,j)} - DT^{t_{x+1}}_{(i,j)})$ for the different time slots t_x.

$ER_{(i,j)}$ is the event-related honesty, and it represents the rate of non-existent events reported by j to the total number of events reported by that same node in a period of time t. Since j is a direct neighbor of i, we assume that i can verify, after a short period, if vehicle j has broadcasted a real or a fake event report. Equation 10 shows how $ER(i,j)$ is computed based on the different

periods evaluated (equation 9):

$$ER^{t_x}_{(i,j)} = \Big[\frac{\sum j's\ \#fake\ events}{\sum j's\ \#events}\Big]^{t_x} \tag{9}$$

$$ER(i,j) = \frac{\beta \cdot \Big[\frac{\sum_{x=1}^{n-1} ER^{tx}_{(i,j)}}{n-1}\Big] + ER^{t_n}_{(i,j)}}{\beta + 1} \tag{10}$$

Finally, $RC_{(i,j)}$ is the evaluation of i about the recommendations (RC) that j has broadcasted within its beacons. If the number of negative recommendations is excessive (e.g., more than 50% of the generated recommendations), this event will be considered as an attempt to perform a bad mouthing attack. $RC_{(i,j)}$ will be equal to the number of negative recommendations (< 0.5) divided by the total number of recommendations. Equation 11 summarizes the recommendations evaluation:

$$RC(i,j) = \frac{\sum j's\ \#negative\ rc}{\sum j's\ \#rc} = \frac{Card\{Opinion(j,k) < 0.5\}}{Card\{Opinion(j,k)\}} \forall k \tag{11}$$

In addition, to improve the risk evaluation procedure, we associate to each parameter (DTV, ER, RC) in equation 7 a factor representing the influence of every report compared to the two other parameters. For example, if a node launches a betrayal attack, its DTV will be much higher than ER and RC, and, therefore, the DTV report should have more weight than the other reports. To this end, in equation 7, DTV is multiplied by $\frac{DTV}{DTV+ER+RC}$, ER by $\frac{ER}{DTV+ER+RC}$, and RC by $\frac{RC}{DTV+ER+RC}$.

5. Multi-hop information dissemination using RITA

Multi-hop dissemination is used mainly for alerting vehicles and authorities on the road about a safety event. However, multi-hop dissemination is also used for data message propagation.

Using the global trust evaluation, any vehicle i can judge any neighbor j and, hence, accept or reject interactions with this neighbor. As mentioned above, a

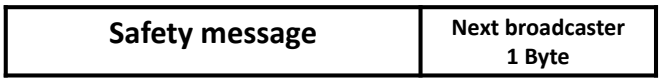

Figure 4: Safety message extension.

trust threshold can be chosen according to the system security requirements or context-based information; for instance, in safety cases this threshold should be low since it is a critical case. Thus, a decision about a vehicle 'j' can be made following equation 12:

$$\begin{cases} j \text{ is a trusted neighbor} & If\ GT(i,j) \geq TrustThreshold \\ j \text{ is an untrusted neighbor} & Otherwise \end{cases} \tag{12}$$

Since most VANET applications, such as Internet access, electronic payment, service discovery, and parking place booking, rely on Road Side Units (RSU) for communications [29], the aim of multi-hop data message dissemination in these intelligent transportation systems services (ITS-s) is to reach the closest RSU in a reduced period of time. Thus, we distinguish between two dissemination types: (i) safety messages dissemination, and (ii) data messages dissemination, in order to ensure a fast delivery of safety messages, and a high efficiency with low packet loss in infotainment scenarios.

5.1. Multi-hop dissemination of safety messages

Same as beacons, we propose to extend safety messages with an additional field containing a pre-selected next broadcaster of the safety message, this way we avoid broadcast storms, as well as network resource exhaustion (see figure 4).

The next broadcaster in every hop is selected in a way so that it is the farthest trusted neighbor, thereby maximizing the additional coverage area [30, 31]. For every neighbor j the vehicle i associate a score $Score(i,j)$ representing a balance between the global trust $GT(i,j)$ and the distance $Distance(i,j)$ between i and

j as shown in equation 13

$$Score(i,j) = \frac{GT(i,j)}{Distance(i,j)} \tag{13}$$

Equation 14 shows the selection procedure of a next broadcaster j among the neighbors of a vehicle i:

$$NextB = j \ / \ Score(i,j) = Max\{Score(i,j),\ \forall\ j \in Neighbors\ of\ i\} \tag{14}$$

Where {k, ..., N} are the current neighbor identities for vehicle i.

Once the re-broadcasting is done, vehicles receiving the same safety message can again drop it and remove the saved version of this safety message as well. Moreover, in the case of a broadcasting failure including both link-related and threat-related reasons, one of the informed vehicles should take the broadcasting decision. In addition, the neighbors of a vehicle 'i' are not necessarily neighbors of each other. Hence, even if the next broadcaster selected (green car with rectangle in figure 5) broadcasts the safety message, we can still have some neighbors that remain uninformed about this action. The latter should rebroadcast safety messages to cover other non-informed zones once its waiting time has expired without receiving another copy of the safety message. To this end, upon receiving a safety message, every neighbor j sets a timer according to the distance to the safety message's source i and accounting for the communication range.

Equation 15 describes how this waiting time can be computed:

$$WaitingTime = DistanceT(i,j) + TT + PT + PRT \tag{15}$$

In this equation $DistanceT(i,j)$ refers to the distance-based waiting time, such as in [32, 33, 34], and it is used in such a way that the farthest neighbor will have the shortest waiting time. TT, PT, and PRT correspond to the maximum Transmission, Propagation, and message PRocessing Times, respectively.

Algorithm 1 summarizes the safety messages' multi-hop dissemination procedure. When vehicle i receives a safety message sent by another vehicle j, it

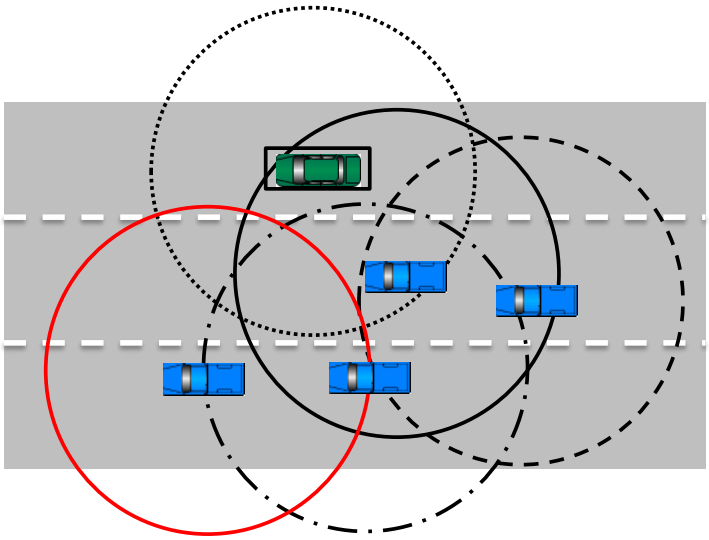

Figure 5: Per-vehicle dissemination areas.

checks the global trust $GT(i, j)$. If it is lower than a predefined threshold, the safety message will be dropped because j is considered to be an untrusted vehicle. Otherwise, the broadcasting process should continue since 'j' is considered to be a trusted neighbor.

Afterward, if i finds its identity piggybacked within the safety message, this means that it is the one selected as next-hop broadcaster. In addition, if the piggybacked identity is not even part of i's neighbors list, it verifies the safety event validity, selects the next broadcaster, and rebroadcasts the safety message. However, if the safety event's validity expires, the latter will be logically canceled. Otherwise, if i is not the selected vehicle for rebroadcasting the safety message, and if its waiting time has expired without receiving another copy of the safety message, it selects a new next broadcaster to broadcast the safety message.

Algorithm 1 Safety messages multi-hop dissemination

```
1: Upon receiving a safety message by i sent by j;
2: if (GT(i, j) ≥ TrustThreshold) then
3:     if ('i' is the next broadcaster OR next broadcaster ∉ neighbors list of 'i' ) then
4:         if NotExpired(safety message, relevance distance, validity duration) then
5:             NextB ← Select next broadcaster (Equation 14);
6:             Broadcast(safety message, NextB);
7:         else
8:             Cancel (safety message);
9:         end if
10:    else
11:        WaitingTime ← Compute waiting time (Equation 15);
12:        if Expired(WaitingTime) AND NotReceived(safety message, NextB) then
13:            NextB ← Select next broadcaster (Equation 14);
14:            Broadcast(safety message, NextB);
15:        end if
16:    end if
17: else
18:    Drop(safety message);
19: end if
20: End
```

5.2. Multi-hop dissemination of data messages

Disseminating data messages among vehicles is a procedure adopted by many VANET applications like delivering ads, restaurant menus, and short-term offers to passing-by vehicles. However, to have a sure and permanent broadcasting of this information, the use of road side units is mandatory. Hence, to preserve the communications bandwidth, vehicle-to-vehicle broadcasting is used only to

reach the RSU.

RITA assumes that vehicles are equipped with a Global Positioning System (GPS), so they can locate vehicles and RSUs within the network. Similarly to safety messages, we assume that we have an additional field containing the selected next forwarder identity as illustrated in figure 3, but with data messages instead of safety messages.

Unlike the safety messages (see equation 14) where the main concern is the delay, the next forwarder for data messages (NextF) is selected using the link duration estimation and distance in addition to the trust between peers in order to minimize both propagation delay and packet loss ratios. For every neighbor j the vehicle i associates a score $Score(i,j)$ representing a balance between the trust $GT(i,j)$, the link duration $LinkD(i,j)$, the distance $Distance(i,j)$ separating i and j, and the distance separating j from the closest RSU $Distance(j,RSU)$ as shown in equation 16

$$Score(i,j) = \frac{GT(i,j) + LinkD(i,j) + Distance(i,j)}{Distance(j,RSU)} \tag{16}$$

Equation 17 represents the next forwarder selection based on the different neighbors' scores:

$$NextF = j \ / \ Score(i,j) = Max\{Score(i,j),\ \forall\ j \in Neighbors\ of\ i\} \tag{17}$$

where {k, ..., N} is the set of neighbors for vehicle i. RSU is the closest roadside unit in the neighborhood which can be easily found using the GPS.

The sum of the global trust given by i to j, the distance between i and j, and the link duration between i and j, is divided by the distance between the neighbor j and the closest RSU, in order to get the closest, trusted and stable path to the RSU, as shown in equation 17.

$LinkD(i,k)$ is the link duration estimation between vehicle i and its neighbor

k, and it is computed according to equation 18.

$$LinkD(i,j) = \begin{cases} \frac{R+Distance(i,j)}{|V(i)-V(k)|} & If\ V(i) \geq V(k) \\ \frac{R-Distance(i,j)}{|V(i)-V(k)|} & Else \end{cases} \tag{18}$$

In this equation R refers to the communication ratio, and $V(i)$ is the speed of vehicle i. Algorithm 2 summarizes the data messages forwarding process.

When a node i receives a data message forwarded by another node, it first checks whether it was selected as the next forwarder for that message. If so, it continues the forwarding process. Otherwise, the processing that follows depends on the application type, thus being outside the scope of this paper. Afterward, if the data message sender had a higher trust than the predefined threshold, the current node tries to reach the RSU if it is within communication range. Otherwise, it selects the next forwarder and then it forwards again the data message. Obviously, the message will be dropped if i considers j to be untrusted.

Algorithm 2 Data messages multi-hop dissemination.

```
Upon receiving a data message from j by i;
if (i is the next forwarder) then
    if (GT(i, j) ≥ TrustThreshold) then
        if ∃ RSU ∈ neighbors of i then
            Forward(msg) to RSU;
        else
            NextF ← Select next forwarder (Equation 17);
            Forward(msg, NextF);
        end if
    else
        Drop(msg);
    end if
end if
End
```

Figure 6: Simulated scenario of Laghouat city, Algeria.

6. Performance evaluation

To evaluate our *RITA* architecture we relied on the NS-2 simulator [35] modified to consider the IEEE 802.11p standard. The generated vehicular traffic is based on the Citymob mobility model [36], which uses SUMO [37] to create mobility traces based on real maps extracted from OpenStreetMap using the Krauss Mobility model [38]. In our case we used a map from the downtown area of Laghouat, Algeria (see figure 6).

Table 1 summarizes the main simulation parameters:

Table 1: Simulation parameters.

Parameters	Value
Simulation area (km×km)	2×2
Simulation time (s)	300
Transmission range (m)	300
Permissible lane speed (km/h)	[0,80]
Number of vehicles	{100, 200, 300, 400}
Dishonest vehicles presence (%)	{15, 25, 35, 45}
TrustThreshold	0.5
W (s)	100
P (s)	2
β	0.7

We divide our experiments into three parts: first, we address the optimal selection of our time window and its time slots, as well as the trade-off between trust and risk information. Second, we compare the performance of our proposal against two other existing proposals - T-CLAIDS [14] and the AECFV [15] - in different scenarios. While the AECFV proposal is dealing mainly with blackholes, the authors of T-CLAIDS did not detail their adversarial model, only assuming the attacker to have a stable continuous malicious behaviour. Finally, in the third part we discuss our proposed messages dissemination technique effectiveness taking end-to-end delay and packet loss ratio as the target metrics.

In our scenario, we assume that beacons are exchanged every half a second, while an event (i.e. safety message) occurs every 10 seconds.

6.1. Determining the optimal parameter settings

In this section we will determine the optimal values for the α factor representing the trade-off between the inter-vehicular trust and the risk estimation, allowing to defend against both standard and intelligent attacks. In addition,

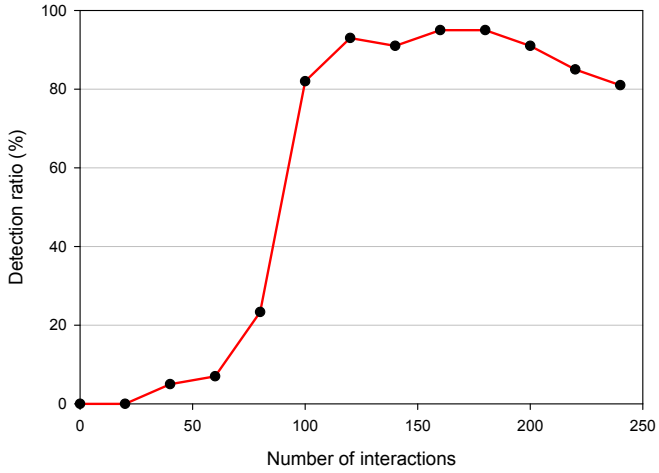

Figure 7: Required number of interaction for an efficient trust establishment.

we discuss the choices for the W and P which refers respectively to the window size and the slots duration parameters. Initially, we assume that factor $\alpha = 0.6$, and that 25% of the vehicles within the network are dishonest and behave as blackholes.

Figure 7 represents the dishonest nodes detection ration with respect to the number of interactions (safety and data messages + the recommendations piggybacked to the received beacons), we note that the detection ratio increases until we reach approximately 100 interactions when it then offers almost a stable values. Therefore, our solution can converge to its optimal detection ratios after approximately 100 interactions.

In addition, while varying the number of vehicles within the network, figure 8 shows that the average number of direct neighbors is also an important factor in the detection process, and that it is logically related to the amount of inter-vehicle interactions shown in figure 7. Furthermore, figure 8 also shows that the average number of direct neighbors should not be below 2, otherwise, our proposal would not perform as good as expected.

As result, the size of W and P can be selected dynamically based of the num-

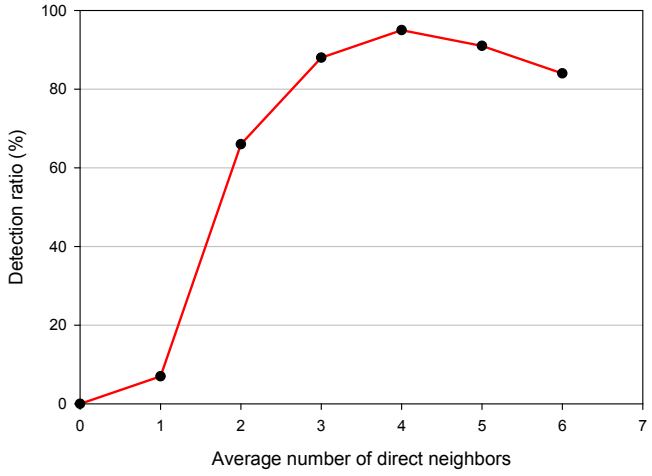

Figure 8: Required number of neighbors for an efficient trust establishment.

ber of interactions if we assume that all vehicles can chose different standards, with different beaconing frequency, or based on a combined value (number of direct neighbors, synchronization delay). Hence, we will have an interactions-based or a neighbors-based selection of values for W and P.

Moreover, many other factors can be taken into account such as: vehicle density, the simulated map (urban or freeway), as well as the communication range. Thus, artificial intelligence solutions such as neural networks can be used to estimate the best values of W and P dynamically.

For the experiments that follow, we pick the best settings, resulting in $W = 100s$ and $P = 20s$. These values are achieved for a beacon frequency equal to 2 Hz (i.e, 2 beacons per second), and considering that a data message is sent by every vehicle each $10s$.

As discussed is section 4, factor α represents the trade-off between the inter-vehicular trust and the risk estimation, and so it can take different values to achieve different trade-offs. Figure 9 represents the detection ratios while varying α parameter. The resulting histograms for different values of α refers to the detection performances of RITA againt the intelligent attack, the bad mouting

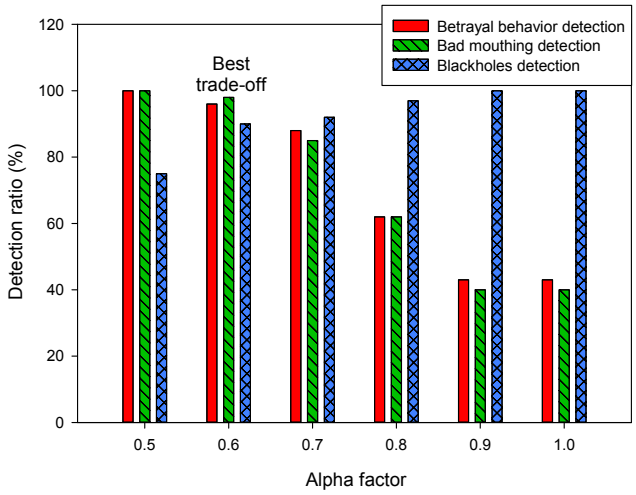

Figure 9: α factor selection.

attack, and the blackholes attack. It becomes clear from the histograms that the best trade-off in terms of detection of the three suggested attacks - betrayal, bad mouthing and blackholes - is achieved for $\alpha = 0.6$.

Furthermore, our system alternates between $\alpha = 0.6$ (combined trust and risk) if one of the risk estimation parameters is higher than a predefined threshold TH and $\alpha = 1$ (trust without risk) if there is no behaviour changing by an intelligent attacker (the risk estimation parameters are lower than a predefined threshold TH) as described in equation 19:

$$\alpha = \begin{cases} 0.6 & If\ (DTV\ Or\ ER\ Or\ RC) \geq\ TH \\ 1 & Otherwise \end{cases} \tag{19}$$

Same as $TrustThreshold$ of equation 12, the TH threshold can be chosen according to the system security requirements. Hence, for both event related (ER) and direct trust variation (DTV), this threshold should be low (e.g, 0.3) since it is refers to a safety critical case or a detection skip tentative. Higher values of TH can be acceptable for the case of false recommendations (RC) since we give more importance to the direct trust evaluation than the indirect

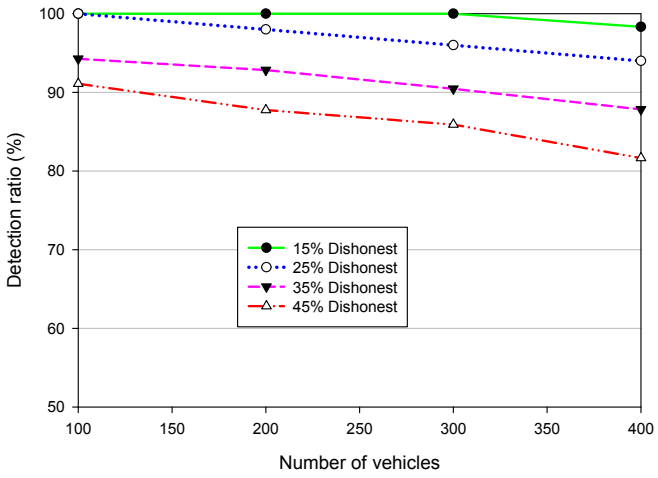

Figure 10: *RITA* detection performance for different vehicular densities in the presence of intelligent attackers.

one.

6.2. RITA attackers detection performance

In this section we show *RITA*'s dishonest vehicles detection performances in the case of intelligent attackers that behave according to figure 1. Afterward, under a continuous dishonest behaviour, we compare our *RITA* proposal against two existing proposals: T-CLAIDS and AECFV.

Figure 10 represents the detection ratios of *RITA* with respect to the number of nodes. It shows that, when varying the number of vehicles in the network, our proposal can offer good detection ratios mostly exceeding the 90%. In fact, even for extremely high ratios of attackers (45%), the detection ratio remains above 82%. The performance levels for more realistic attacker ratios ($\leq$ 15%) are nearly 100%, despite all of them perform intelligent attacks thanks to the risk estimation that allows to *RITA* detecting such behaviour.

In addition, we compared our solution against other proposals such as AECFV and T-CLAIDS. As discussed in sections 1 and 2, it should be noted that the

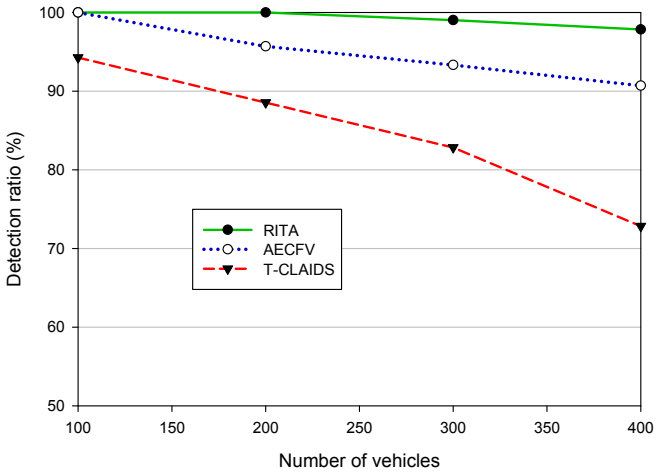

Figure 11: Detection performances compared to AECFV and T-CLAIDS for different densities (35% dishonest vehicles).

latter are only able to detect blackhole attacks, being unable to deal with attackers endowed with trust establishment awareness, and able to launch intelligent attacks, which raises the detection complexity. Thus, we have simplified the adversarial model to blackhole attacks alone, meaning that attackers will merely send negative recommendations about its direct neighbors. Figure 11 represents the detection ratios for different densities of vehicles. It shows that our proposal clearly outperforms T-CLAIDS and AECFV by more than 4% for a density higher that 300 vehicles. Here, since non of the risk estimation parameter have a high value exceeding the threshold TH discussed in the previous section, the α parameter is equal to 1. Hence, the risk estimation margin of error is avoided.

Figure 12 represents the detection ratios for different attacker ratios when the number of vehicles is set to 400. Similarly to figure 11, figure 12 shows that, when varying the ratio of dishonest vehicles in the scenario, $RITA$ is able to perform better than both AECFV and T-CLAIDS, ensuring high detection ratios (>90%) even if almost half (45%) of the vehicles are dishonest.

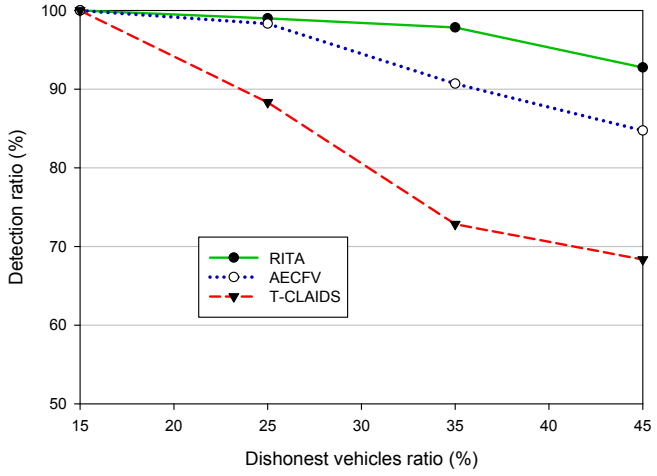

Figure 12: Detection performances compared to AECFV and T-CLAIDS for different dishonest vehicles ratios (400 vehicles scenario).

6.3. RITA messages delivery performance

We now study the effectiveness of the proposed dissemination technique in the presence of dishonest vehicles in the network. Since the message delivery process attempts to reach an RSU in the shortest possible time, we also assess the impact of varying the RSUs density among: (a) 3 RSUs, (b) 6 RSUs, (c) 9 RSUs, and (d) 12 RSUs as illustrated in figure 13.

Figure 14 represents the average end-to-end delay required for packets to reach an RSU when varying the number of vehicles and RSUs in the network. The resulting histogram shows that, except for the case of low vehicle and RSU densities (less than 200 vehicles and less than 6 RSUs), our proposed technique is able to provide low delays to the message delivery process (≤ 1 *second*) despite the high attackers ratio (35%). For lower attacker ratios, results are even better.

Concerning the packet loss ratio, figure 15 shows that -similarly to the average end-to-end delay- and thanks to the best forwarder/broadcaster selection, our solution can overcome the high ratio of attackers (35%) and ensure low packet loss ratios, especially under high levels of connectivity (number of vehi-

Figure 13: RSUs distribution in the simulated scenario of Laghouat city, Algeria.

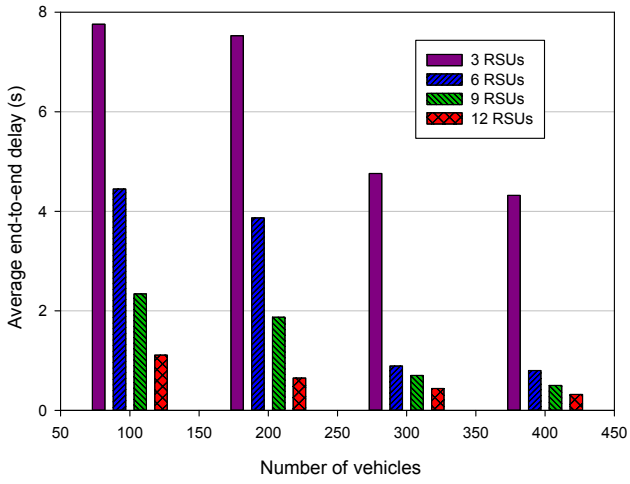

Figure 14: Average end-to-end delay required to reach an RSU for different vehicle and RSU densities (35% of dishonest vehicles).

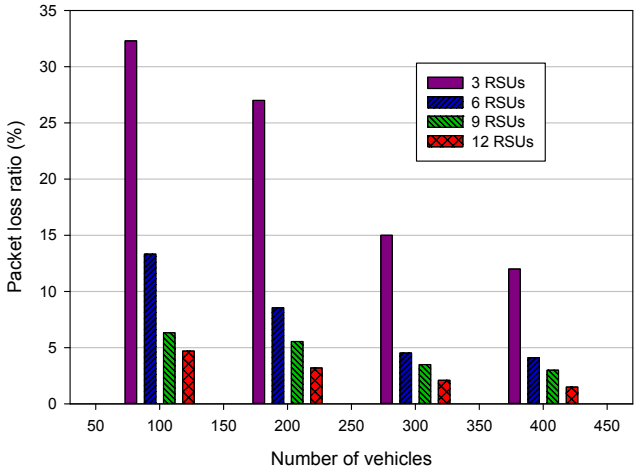

Figure 15: Packets loss ratio for different vehicle and RSU densities (35% of dishonest vehicles).

cles higher than 200) and the presence of a significant number of RSUs (6 or more), and can reach quasi optimal values (less than 3%) for a dense network of both vehicles and RSUs (respectively more than 300 vehicle and 12 RSU).

7. Conclusions and future work

Introducing security enhancements in collaborative networks is always a hard and challenging task. In addition, highly dynamic environments like VANETs make the problem even more complex. The assumption that all nodes are honest and collaborative can lead to catastrophic damages, especially in the scope of safety applications. With these challenges in mind, in this work we presented a trust-based risk-aware technique able to sustain collaborative inter-vehicular communications even in the presence of high ratios of intelligent attackers within the network. Our proposal, called *RITA*, can set dishonest vehicles aside from all network operations in a completely distributed manner, which makes it independent from the environment and applicable both in the presence and absence of RSUs.

Simulation results have shown $RITA$'s ability to ensure high detection ratios exceeding the 90% even for a high presence ratios of attackers (45%), as well as short end-to-end delays (< 0.5s) and reduced packet loss ratios ($< 3\%$) for a scenario of more than 300 vehicles and 9 RSUs.

As future work, we plan to study some other types of adversaries adopting pseudonym-changing techniques for malicious purposes. We also plan to take advantage of the possible deployment of a Public Key Infrastructure (PKI) to enhance the inter-vehicular trust accuracy.

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] I. A. Sumra, I. Ahmad, H. Hasbullah, J.-l. B. A. Manan, Classes of attacks in vanet, in: Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International, IEEE, 2011, pp. 1–5.

[2] 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.

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

[4] A.-S. K. Pathan, H.-W. Lee, C. S. Hong, Security in wireless sensor networks: issues and challenges, in: Advanced Communication Technology,

2006. ICACT 2006. The 8th International Conference, Vol. 2, IEEE, 2006, pp. 6–pp.

[5] 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.

[6] S. Chen, Y. Zhang, Q. Liu, J. Feng, Dealing with dishonest recommendation: The trials in reputation management court, Ad Hoc Networks 10 (8) (2012) 1603–1618.

[7] V. Bibhu, K. Roshan, K. B. Singh, D. K. Singh, Performance analysis of black hole attack in vanet, International Journal of Computer Network and Information Security (IJCNIS) 4 (11) (2012) 47.

[8] 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.

[9] 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.

[10] 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.

[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] 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.

[17] 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.

[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] C. A. Kerrache, N. Lagraa, C. T. Calafate, A. Lakas, Trouve: A trusted routing protocol for urban vehicular environments, in: Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on, IEEE, 2015, pp. 260–267.

[20] Etsi eurpean standard, en 302 637-2 - v1.3.1, (2014-09).

[21] 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.

[22] K. C. Abdelaziz, N. Lagraa, A. Lakas, Trust model with delayed verification for message relay in vanets, in: Wireless Communications and Mo-

bile Computing Conference (IWCMC), 2014 International, IEEE, 2014, pp. 700–705.

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

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] D. Chkliaev, J. Hooman, E. De Vink, Verification and improvement of the sliding window protocol, in: Tools and Algorithms for the Construction and Analysis of Systems, Springer, 2003, pp. 113–127.

[29] S. Olariu, M. C. Weigle, Vehicular networks: from theory to practice, Crc Press, 2009.

[30] D. Li, H. Huang, X. Li, M. Li, F. Tang, A distance-based directional broadcast protocol for urban vehicular ad hoc network, in: Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on, IEEE, 2007, pp. 1520–1523.

[31] W. Viriyasitavat, F. Bai, O. K. Tonguz, Uv-cast: an urban vehicular broadcast protocol, in: Vehicular Networking Conference (VNC), 2010 IEEE, IEEE, 2010, pp. 25–32.

[32] A. Bejan, R. Lawrence, Peer-to-peer cooperative driving, in: Proceedings of ISCIS, 2002, pp. 259–264.

[33] J. Bronsted, L. M. Kristensen, Specification and performance evaluation of two zone dissemination protocols for vehicular ad-hoc networks, in: Proceedings of the 39th annual Symposium on Simulation, IEEE Computer Society, 2006, pp. 68–79.

[34] S. Dornbush, A. Joshi, Streetsmart traffic: Discovering and disseminating automobile congestion using vanet's, in: Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th, IEEE, 2007, pp. 11–15.

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

[36] 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.

[37] 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.

[38] D. Krajzewicz, G. Hertkorn, C. Rössel, P. Wagner, Sumo (simulation of urban mobility)-an open-source traffic simulation, in: Proceedings of the 4th Middle East Symposium on Simulation and Modelling (MESM20002), 2002, pp. 183–187.