Securing Vehicular Networks based on Data-Trust Computation

Sînziana Mazilu[*], Mihaela Teler[*], Ciprian Dobre[*1]
[*]*University POLITEHNICA of Bucharest, Romania*
E-mails: {sinziana.mazilu, mihaela.teler}@cti.pub.ro, {ciprian.dobre}@cs.pub.ro

Abstract

Vehicular ad-hoc networks (VANETs) have a great potential to improve road safety, traffic jams, fuel consumption, and to increase passenger convenience in vehicles. However, VANETs use an open medium for communication and, therefore, are exposed to security threats that influence their reliability. We propose a data-trust security model designed for VANETs based on social network theories. Drivers receiving data about traffic congestion or safety warnings can use the model to evaluate the trust in the received information. The model computes a trust index for each message based on the relevance of the event. It also uses a gossiping approach to disseminate data-trust indexes between vehicles, increasing the accuracy in the trustworthiness of an event and assuring the privacy by hiding the original event sources. The approach is evaluated through modeling and simulation, and we present results that proof its validity.

Keywords: vehicular networks; security; privacy; data trust computing; trust indexes.

1. Introduction

Vehicular Ad-Hoc Networks (VANETs) [13] are particular wireless networks formed when equipping vehicles with short-range wireless communication devices. Potential VANET applications can lead to improved road driving conditions, less pollution, safety in driving, increased comfort for passengers and many others [4]. However, VANET applications for collision-warnings and congestion avoidance need mechanisms to evaluate the trust in the data collected by other vehicles [6, 7]. For this reason current research topics in VANETs include mechanisms for providing secure communication, and verification of data against malicious attackers [12, 13].

Such mechanisms should also preserve privacy of passengers. Privacy is, in the context of secure communication in vehicular networks, a major challenge [8]. Except for the case of economic models, in VANETs drivers willingly participate in the communication. For example, they might help to monitor and forward current road conditions, forward emergency messages, etc. But the driver also needs guarantees that, unless he/she does something illegal, his/her identity is not used against himself, *e.g.* for phishing and other attacks.

We propose a solution to secure vehicular networks using data-trust computation and social network theories. The solution preserves the privacy of the VANET users by hiding the original event sources.

Our contribution is twofold. First, we propose a solution to the security problem using social network theories [11]. Each driver computes a trust index for each event using the context information encapsulated in the corresponding message. The context data describes when and where a particular event was produced, or how many vehicles forwarded the message. The trust index is then compared with the information received from other drivers relative to the same event. The approach uses gossiping-based dissemination to improve the accuracy of the trust value. This works because vehicles in movement tend to follow specific social network patterns [2]. Second, we evaluate the proposed solution by modeling and simulation. We present evaluation results for simulation scenarios where vehicles communicate to report events for road conditions, safety warnings, traffic info updates (e.g. traffic jam), accident reports, weather reports (e.g. ice on road). We show how our data-trust based approach successfully prevents attacks like message alteration, message fabrication, message suppression and cheating with identity [4].

The remainder of the paper is structured as follows. Section 2 contains a brief related work on security and privacy in VANETs. In Section 3 we present the architecture of the data-trust system. Section 4 details the proposed mechanism to compute the data-trust in VANETs. In Section 5 we give a complete description on the implementation details of the proposed security solution as an extension of the VNSim simulator, together with the experimental setting and evaluation of results. Section 6 concludes and presents future work.

[1] The research presented in this paper is supported by national project: "TRANSYS – Models and Techniques for Traffic Optimizing in Urban Environments", Contract No. 4/28.07.2010, Project CNCSIS-PN-II-RU-PD ID: 238. The work has been co-funded by the Sectoral Operational Programme Human Resources Development 2007-2013 of the Romanian Ministry of Labour, Family and Social Protection through the Financial Agreement POSDRU/89/1.5/S/62557.

2. Related Work

Various authors analysed how traditional security solutions can be applied in VANETs [6, 12, 13]. Such solutions include certificate based systems, Kerberos, pseudonyms, blind signatures, digital credentials, group signatures, etc. However, they tend to rely on the existence of a security infrastructure and on common, global, trusted and well-known system parameters and entities (e.g. the existence of a centralized CA) used for message authentication. This is why currently authors tend to agree that security in VANETs is better approached through trust mechanisms [4, 14, 16]. Trust-based systems avoid the use of the central authority that is used in traditional systems as the trusted entity that can make guarantees. A central authority cannot be easily accessed and managed in dynamic highly mobile wireless environments such as VANETs.

Wex, *et al* [10] identifies the need to use self-organizing mobile architectures to evaluate the trust in VANETs. In this case the security trust-based system must consider two characteristics of VANETs: 1) there is no trusted third party such as a supervisor infrastructure involved, and 2) there is no global knowledge shared among the participating nodes. The authors suggest the use of self-organizing trust establishment methods used in the context of VANETs. They propose the use of CONFIDANT as a protocol to detect and isolate uncooperative nodes, Terminodes for coping with selfish nodes in the network, SPRITE (similar to Terminodes, but uses credits to encourage selfish nodes to cooperate), and Location Limited Side Channels to isolate the suspicious node so the attacker cannot gain physical access to the communication channel. We agree that in VANETs trust is hard to be computed using a centralized certification infrastructure. However, in our case trust is computed ad-hoc using the context conditions that led to the production of a specific event. In addition, we use a gossip-style approach, and also present validation results of the solution using modelling and simulation.

Boukerche&Ren [1] present a trust-based security system, TOMS (Trust cOmputation and management System), used to establish a set of effective rules to make reliable analysis of certain suspicious nodes. It is based on distributed and incomplete information and considers the dynamic and flexible nature of the topology. The author introduce the concept of community (or group), consisting of a central node and a set of one-hop neighbouring nodes that might contain malicious nodes (a simplified version of the community concept used in social networks [11]). Each node has its own community centred at itself in the trust management system. The authentication between the central node and its neighbours is accomplished using cryptographic techniques. However, such an approach might be appropriate for MANETs, but proposed mechanism to compute trust indexes is not suitable for VANETs, because of the increased node mobility.

Raya *et al* [7] argue that the traditional notion of trust becomes insufficient for emerging data-centric mobile ad-hoc networks. The challenge is to extend the traditional notion of trust to data-centric trust. The validity of data is inferred by a decision component based on one of several evidence evaluations techniques (majority voting, most trusted report, Bayesian inference, Dempster-Shafer Theory). Then a trust factor for each piece of data is computed individually, considering possible contradictions in information relative to a common event. In this context, Stumpf *et al* [9] present a multi-layered security protocol that allows a vehicle to receive certificates used for transferring traffic safety messages, while privacy of nodes is protected. The protocol combines different types of signature schemes (RSA signatures, DSS). It uses SRAAC (Secure Anonymous Authenticated Inter-Vehicle Communication), a scheme based on distributed magic-ink signatures. Unlike similar blinded signature schemes [5], the approach provides the possibility to unblind a signed message.

Security of mobile ad-hoc networks domain is carried out by different organizations (e.g., Car 2 Car Communication Consortium in Europe [15]). Still today no mechanism can provide security guarantees in VANET environments. Current solutions to security issues in VANETs are still in an early stage of development. In this context the data-trust computation model proposed in this paper represents an alternative to compute the trust indexes in VANETs. Unlike other solutions, we propose a deterministic model that uses context to filter faulty messages. The approach also ensures privacy of participants by validating each event disregarding the identity of the source vehicle.

3. System Architecture

Many applications deployed in a VANET require the use of security mechanisms. We propose the addition of a component sitting between the communication infrastructure and VANET applications (Figure 1). This facilitates the use of the proposed security mechanisms in already existing VANET environments, because the component acts as an independent layer that is able to transparently handle security aspects and filter correct message from malicious or faulty ones. It does not interfere with the business logic of the application and/or with the communication primitives.

The messages received from the wireless environment enter the security module. Then trust indexes are computed for each individual message containing information about events. The trust index is next evaluated and only the trusted data is forwarded above, to applications.

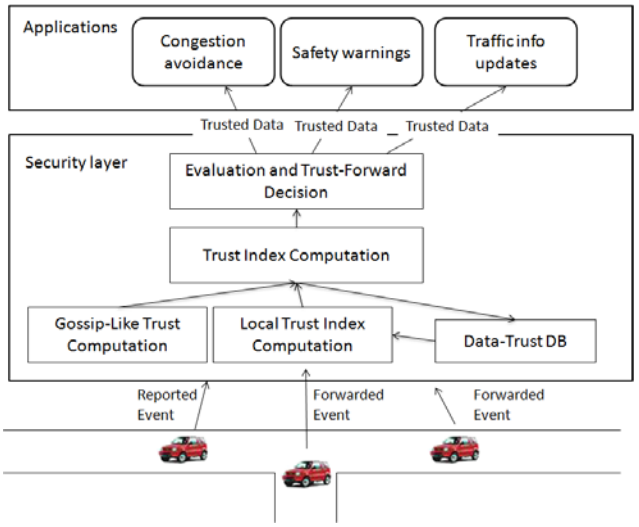

Fig. 1. The security architecture.

There is no overhead that could impact the performance of the communication network, because the trust index is computed locally on each node (we collectively refer to the car and its computational device capable to run locally a VANET application as a *node*).

The information relative to an event is encapsulated in a security message. This message contains additional context information (time, location). When a message is received its trust index is first analyzed. For that the vehicle uses the database (*Data-Trust DB*) containing messages reporting observations relative to the same event, and the trust index is updated according to a trust-computation rule by the *Trust Index Computation* component. The trust index is locally computed by the *Local Trust Index Computation* component. Also, this component verifies if the local vehicle is capable of confirming the event based on local observations. The index is updated based on observations coming from cars located in the vicinity of the event, at a moment relatively close to when the event was produced. The *Gossip-Like Trust Computation* component implements the logic of disseminating information when possible to better filter faulty events. If the trust index is greater than a threshold, the message is further forwarded to the wireless network. Otherwise the message is discarded, therefore eliminating further propagation of incorrect observations. This is accomplished by the *Evaluation and Trust-Forward Decision* component.

We further analyzed several methods for computing the trust indexes and investigate how they perform under various traffic conditions. The solution is based on the observations received from the majority of drivers. The context information is guaranteed by trusted entities and the approach is described in the next Section. Then, for computing the trust index, each node keeps a database with messages received in the last period of time from the neighbouring nodes. The database also contains trust indexes for each record.

4. Trust index computation

In this section we will give a brief description of the security protocol in which our approach is integrated and we will describe our proposed methods.

4.1. The security protocol

To guarantee the context (the location where it was produced, the time when it was produced) in which specific events were produced, and also their correct dissemination, we assume the use of a security communication protocol [3]. The protocol ensures privacy, integrity, availability, and non-repudiation (these properties were previously explored in [3], to which we refer the reader for further background information). As it is used for securing communication in VANETs, the protocol considers the existence of several entities (see Figure 2): *secure cars* (SC) and *secure traffic lights* (STL).

To secure the transmission of messages between nodes the protocol assumes the existence of certification authorities presented in different locations. It can be a traffic light equipped with an access point and connected to a server (the *secure traffic light* in Figure 2).

The *secure car* is considered a mobile entity that exchanges messages with other traffic participants, but also with the existing infrastructure (i.e. secure traffic lights). The communication protocol provides a solution to secure messages such that to allow the destination to verify their legitimacy. In this sense STLs act as certifying entities that help secure cars prove the legitimacy of received messages.

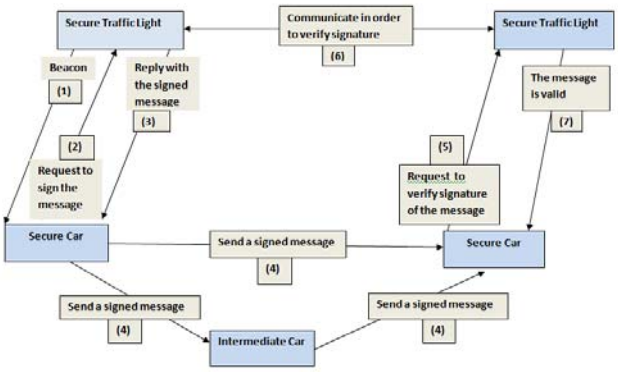

Fig. 2. The security protocol.

When an SC wants to send a message it stores it locally until it receives a beacon from a STL. This signaling mechanism is used to ensure that SC transmits the event

from a location that can be further confirmed by a trusted entity (the STL continuously emitting the beacon). Once a beacon is received, the SC sends the message to the STL, which further signs it. The relevant information contained in the message consists of the timestamp and location where the message was produced, followed by the actual payload data. This information is validated and signed (payload, together with position and timestamp) by the STL.

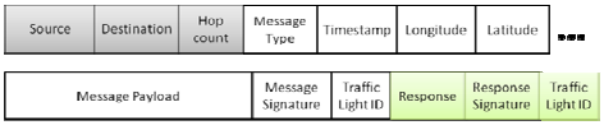

Fig. 3. The structure of a message.

When the SC receives the message augmented with the signature, it further sends the packet to the destination SC. The transmission of the signed message is accomplished in several ways. If the destination is in the wireless transmission range of the source SC, then the message is sent directly. Otherwise, the message is routed through existing intermediate cars to its final destination. Once the message reaches its destination, the destination SC validates it. For this it sends the message to the nearest local STL. The STL verifies the signature of the message, and performs data validation. The result of this verification is sent back to the SC which requested the validation. If the answer is positive, the message is further sent to the application.

The protocol considers messages composed of several fields (see Figure 3). 'Traffic Light ID' holds the identity of the fixed entity that signed the message. This field is used at the other end of the communication for requesting the corresponding public key used in the validation process. The location ('Longitude' and 'Latitude') and 'Timestamp' fields certify the context of the message. Common attacks are based on the fact that users are tempted to lie regarding their geo-position or time when they transmit specific information. Based on these fields an SC can decide to accept or reject a particular message. Messages, regardless of their type, contain the 'Hop count' field to prevent additional message routing.

4.2. The computation of trust indexes

The proposed method for computing data-trust indexes is different from previous approaches based on the trustworthiness of nodes. Such solutions fail to preserve privacy. They use attributes necessary to take decisions based on the credibility and relevance of the nodes, coupled with data consistency. As opposed to that, we propose using the *trust of the data*, meaning the validity of the information. We propose the use of the semantics of the data, and correlate it with observations from neighbour nodes relative to the produced event. A similar idea is proposed in [7]. However, the authors propose a solution based on probabilistic computation of trust indexes. We argue that a better solution can be based on the use of deterministic schemes. Probabilities cannot guarantee a high success rate, a characteristic crucial when dealing with life-or-death applications for safety warnings in VANETs.

The idea is to analyze several messages and deduce information about the validity of an event. We consider the existence of several correct messages to compensate for the misleading messages. We propose the use of the security protocol previously described, or any alternative solutions (*e.g.*, the use of asymmetric keys, periodically exchanged, to assure the privacy of participants), to avoid attacks like the Sybil attack or message replay [9].

The proposed security model assumes that a node having knowledge of a specific event sends reporting messages (ice on road, traffic jams, etc.). Such a message receives a default trust value encapsulated as a field within. Different cars can use different default trust values. A police car or an ambulance is more trustworthy than a normal car. Our approach prevents nodes from using any default trust value. Each node must register to a certificate authority (CA – it can be the STL for example, but not necessarily). When the node receives a certificate from the CA, it receives also its default trust value to be used to compute trust values for the messages received. The CA can verify and sign the type of node, and thus the default trust value used by each vehicle.

The message also includes context information, such as the timestamp and location of the event. Cars in the neighborhood that receive the information about the event can further respond by acknowledging or not the event. Each message has to be confirmed by as many cars as possible before the data is considered trusted.

In addition, from the study of vehicle mobility it can be inferred that they have a tendency towards grouping and forming car clusters [2]. Because of the sparse connectivity between nodes specific to VANETs, we further extend the approach using gossiping to further propagate data about an actual produced event. Gossiping is done when a vehicle is inside a car cluster (such as when waiting on a traffic light). In this case, a car can send information about the events it encounters of has found out about, thus helping others compute the trust indexes relative to the produced event.

For computing trust indexes we use the timestamp contained in the message, the number of hops the message was forwarded, and the number of messages reporting on the same event. The trust index value (TV) is computed according to equation (1). The term TV_1 represents the trust value as perceived by the current car, and TV_2 is the trust value reported by others cars for the same event. The coefficient α_1 and α_2 are given by $\alpha_1 + \alpha_2 = 1$.

$$TV = \alpha_1 TV_1 + \alpha_2 TV_2 \quad (1)$$

The first part of the equation considers the expiration of the message. It uses the *indexTrustRatio* (or *iTR*), a value computed by dividing the difference between the time the message travelled between the event observer and the current car, and the timeout value (see equation 2). The value of this ration is higher as the message travels for a longer time, finally exceeding the timeout value. After the timeout, the message is considered less relevant and the trust index is decreased accordingly.

$$iTR = \frac{t_{current} - t_{original}}{timeout} \quad (2)$$

Equation (3) describes the method for computing the local trust index:

$$TV_1 = (1 - iTR) * tV + tVDB \quad (3)$$

In this equation *trustValue* (or *tV*) represents the trust value encapsulated in the received message. The parameter *trustValueFromDatabase* (or *tVDB*) is the trust value computed by the car for the same information, considering previous local knowledge and the recently received messages with data reports of the event. For each event the trust value is computed and locally stored in the database (see Figure 1).

In equation (3) when the message expires *iTR* becomes greater than *1* and TV_1 decreases. If the message is not expired, then the trust index increases according to how recent or old is the message.

The second part of equation (1) uses majority pooling for computation of data-trust:

$$TV_2 = (tVDB * noMess + tV)/(noMess + 1) \quad (4)$$

where *noMess* represents the number of messages reporting on the same event, stored in the database and incremented with each message.

The malicious information is not explicitly discarded, but it is not taken into account when computing new trust indexes. We incrementally compute and update the trust value of the data, based on each new message received reporting on a particular event. Periodically the database is cleaned up by discarding messages that are older than a preset threshold and by discarding messages that are below a preset trust value (these data is not considered trustworthy and thus it is deleted).

5. Performance Evaluation

The evaluation of VANETs poses unique challenges because of the number of nodes needed for a typical scenario and because of the need for a specific vehicle mobility model. A typical evaluation is conducted either in a real-world scenario, with various cars implementing the application, or using simulation and statistical analysis. The second alternative is preferred because of the repeatability and the possibility to model the same solution in a wide range of scenarios.

5.1. Security module implementation

VNSim is a microscopic discrete event simulator successfully used in evaluating VANET related applications [2]. It is designed as a realistic simulator for evaluating the performances of a wide-range of VANET technologies, ranging from wireless networking protocols and dissemination strategies to applications being developed over VANETs. The simulator is composed of two main models: a flow-based vehicular mobility model that considers driver personalities, traffic motions, realistic maps, and a wireless networking model, responsible with the simulation of the networking components and the communication protocols envisioned by a VANET system.

For evaluating the proposed security solution we extended VNSim with the capability to simulate nodes that send and receive information about specific events and compute trust indexes according to the proposed solution. We first classified vehicles in *EMERGENCY_CAR*, *SECURE_CAR* and *DEFAULT_CAR*. Each vehicle has a different weight in the trust index calculation. *EMERGENCY_CAR* is used to represent authority cars such as police or ambulance. *SECURE_CAR* represents public transport vehicles.

In the simulation experiments we used several types of messages: *EMERGENCY*, *WEATHER*, *ROAD*, *CIRCULATION*, and *APPLICATION*. We next introduced a specific message, *Security Message*, which contains specific fields. The fields *typeMessage* and *typeInformation* identify the type of event (as represented in Table 1). The field *dataInformation* correspond to specific data relative to the produced event. The field *location* identifies the location where the event was produced. *noHops* first receives a default value and each time the message is forwarded the field is decremented. When this value decreases below 0 the message is discarded. The field *timestamp* represents the moment of the observation relative to the event. The messages containing old observations are discarded. Finally, the field *trustCoef* represents the trust index attached to each message according to the source vehicle.

5.2. Modelling security attacks

To evaluate the functionality and the performance of the security solution we simulated several attacks scenarios, placing into the network malicious nodes injecting messages with fake information. First we extended the simulation model with the capability to simulate special

vehicles that runs as attackers. We modeled the attacker's behavior as influenced by some motivations. *Greedy* drivers try to convince other drivers that the road ahead is congested by sending misleading messages. For example, a car equipped with a navigator might receive notifications about possible congestions and dynamically adjust its route to the destination. An attacker might send faulty messages to convince other drivers to compute alternative paths and clear the road.

Another type of an attacker is the *snooper*, who tries to identify drivers and use the information to steal their identity. Such an attacker can use the identity to commit frauds or for other commercial purposes. Another attack scenario injects messages with the trust index altered. An attacker car would modify the trust value of all received messages (if the message has a big trust value, this value becomes little and vice versa) and then forwards the message. Finally, we modeled a *terrorist* attacker that tries to harm the network just to prove it is possible. It can also be the model of a terrorist trying to obtain an ambuscade.

All these scenarios consider that the number of fake messages does not exceed the number of legitimate messages (for each fake message at least one positive message must exist to compensate for the misleading information). This consists with real life situations where usually the number of attackers is below the number of other traffic participants.

We assume that all attackers have the default trust value. The nodes with a higher trust value (like police cars, ambulances) are assumed to be honest (so their opinion on an event is valued higher than other observations).

Fig. 4. The scenario map used in the simulation experiments.

To evaluate the proposed security solution we executed several simulation experiments. The simulation scenario resembles the vehicular traffic in the campus of the University POLITEHNICA of Bucharest (see Figure 4). It consists of variable flows of cars (an average of 50 cars/ lane/hour). We were interested in the capability of the model to solve various attacks using the computed trust indexes.

Raya, *et al* [6] identifies three groups of attacks in VANETs: 1) attacks on safety-related applications (attacks leading to accidents); 2) attacks on payment-based applications (leading to financial frauds); and 3) attacks to privacy (all drivers want to avoid being tracked by other drivers). We also extended the simulation model with several types of attacks: Message Suppression Attack, Denial of Service, Fake Information Attack, and Cheating with Identity.

The *Fake Information Attack* covers two aspects. Fake information can be carried either by injecting messages by fabrication, or by injecting messages by alteration. For example an attacker can send malicious data into the network to affect the decisions taken by other drivers. He can try to mislead the drivers to obtain a clear way to destination. The same attack can be used to obtain congestion on a road, or for financial frauds. In the *Message Suppression Attack* a driver can selectively drop packets from the network. For example an attacker might discard the received congestion alerts to prevent the nodes from selecting an alternative path to destination and forcing them to wait in traffic. Finally, in the *Cheating with Identity* attack a driver might try to participate in message exchanges using fake information. In case of a self-provoked accident this attack might be used by the driver to lie about responsibility for the event. The attack can be done by sending information about the accident with fake information about current location, speed or time of event occurrence.

5.3. Evaluation results for the use of trust indexes for attack prevention

We evaluated the efficiency of the security solution using a *fake information* attack scenario. The experiment contains malicious vehicles that inject messages containing fake information. For example a vehicle sends "*congestion*" or "*accident*" messages to determine other cars to compute alternative paths to destination. In this case an attacker wants to convince other nodes that an event was produced. The attacker sends messages containing the information "*accident*".

The trust value associated with the message is set to the default value corresponding to the source. The nodes in the wireless communication range of the attacker receiving the message process the data and compute its trust index. The nodes located in the event's proximity verify the information, and send correction messages containing the information "*clear road ahead*". Such messages contradict the fake information, and help removing the fake information.

With the use of trust indexes attached to all messages exchanged between vehicles we succeeded to prevent this

attack. In this case only a small number of fake messages support the fake event, the trust index is reduced, and thus the event is considered false.

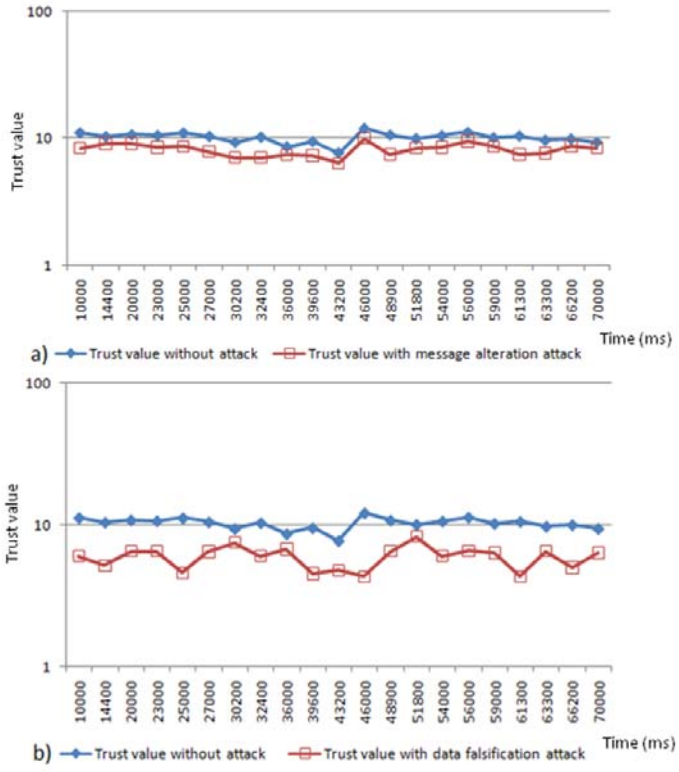

Fig. 5. Evaluation results.

Another attack scenario successfully prevented consists in injecting messages having the associated trust value altered. In this case an attacker modifies the trust value of the received messages and then forwards the message. We conducted several simulation experiments, with and without the attacks, and compared the obtained results. Figure 5 presents the results for the obtained values for trust in these two cases.

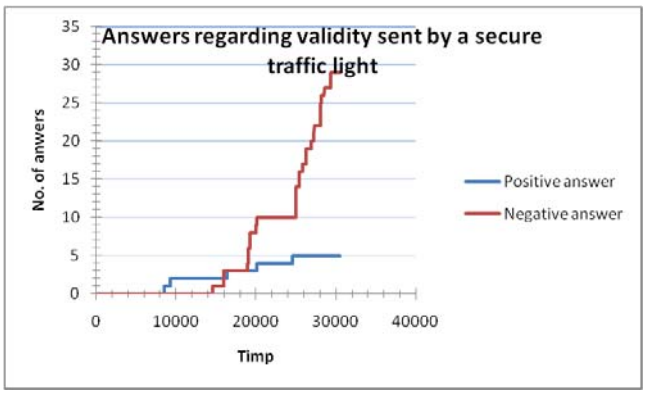

Fig 6. Answers concerning validity sent by the secure traffic light.

As presented, there is a small difference between the trust values obtained when there is no attacker, and for the case where 10% of the vehicles in the network inject fake information (Figure 5a) or messages having altered trust values (Figure 5b). The attacks are successfully resolved, because the fake data is correctly recognized based on the observations coming from proximity vehicles.

We next executed the experiments by increasing the number of attackers (20% of the vehicles), and using various default trust values for the attack cars (*EMERGENCY_CAR*, *SECURE_CAR* and *DEFAULT_CAR*). In all cases the events were correctly identified and the fake information was eliminated.

The security solution was next successfully in preventing the *Message Suppression Attack*. The attack is avoided by setting a threshold for the received number of messages supporting or disproving a certain event before it can be considered to be trusted. With the proposed security solution the *Cheating with Identity* attack is also not feasible because of the secure communication protocol.

The results in Figure 6 correspond to the answers generated by a secure traffic light. We can observe that the secure traffic lights notices that a message is invalid and gives back to the secure car a negative answer (the graphic in red depicts this aspect). Also, we notice that some secure cars received a valid message and this fact is observed in the secure semaphore behaviour (the graphic in blue depicts this aspect). We also executed a series of experiments without any attacker (ideal conditions) and compared the obtained results. The comparison confirms that such an attack does not influence the communication overhead.

6. Conclusion and future work

In this paper we presented a data-trust security model designed for VANETs. Drivers receiving data about traffic congestions or safety warnings can use the model to evaluate the trust in the received information. In this way they are able to evaluate if the message reflects real events or are falsely injected by malicious drivers. In addition the model also ensures the privacy of the drivers.

The contribution consists in the architecture of the trust-based security module and the trust index computation methods explained and evaluated. To ensure that a driver does not cheat regarding to the location and time of the generated or forwarded message, we use a dedicated communication security protocol. Its capabilities were previously extensively demonstrated in [3].

Traditional authentication and access control mechanisms cannot work well in ad-hoc vehicular networks. Unlike previous node-centric models, our model is based on computing a trust index for the data, using context information relevant for the event and assuming participation of proximity cars. We employ the use of a

gossiping approach to disseminate data-trust indexes between vehicles, increasing the accuracy in the trustworthiness of an event and assuring the privacy by hiding the original event sources.

We presented experimental results showing that several attacks, like message alteration, message fabrication, message suppression and cheating with identity, are successfully prevented.

We believe that this paper represents a first step in combining trust-level information with social and context structures and interactions to drive novel and effective means for ensuring trust guarantees in the dissemination of events in VANETs. A great deal of future research can follow.

7. References

[1] Boukerche, A., Ren, Y., 2008. A trust-based security system for ubiquitous and pervasive computing environments. *Computer Communications*, 31(18), pp. 4343-4351.

[2] Gainaru, A., Dobre, C., Cristea, V., 2009. A Realistic Mobility Model Based on Social Networks for the Simulation of VANETs. *In: Proc. of the IEEE 69th Vehicular Technical Conf.* (VTC Spring 2009). Barcelona, Spain, pp. 1-5.

[3] Gosman, C., Dobre, C., Cristea, V., 2010. A Security Protocol for Vehicular Distributed Systems. *In: Proc. of 12th Int. Symp. on Symbolic and Numeric Algorithms for Scient. Comp.* (SYNASC 2010), Timisoara, Romania, pp. 321-327.

[4] Moustafa, H., Zhang, Y., 2009. *Vehicular Networks: Techniques, Standards, and Applications*. Auerbach Publications, pg. 450.

[5] Li, C.-T., Hwang, M.-S., Chu, Y.-P., 2008. A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. *Comput. Commun.* 31 (12), pp. 2803-2814.

[6] Raya, M., Hubaux, J.-P., 2005. The security of VANETs. *In: Proc. of the 2nd ACM international workshop on Vehicular ad hoc networks* (VANET '05). ACM, NY, USA, pp. 93-94.

[7] Raya, M., Papadimitratos, P., Gligor, V.D., Hubaux, J.P., 2008. On data-centric trust establishment in ephemeral ad hoc networks. *In: Proc. of the 28th IEEE INFOCOM*, Phoenix, AZ, pp. 1238-1246.

[8] Studer, A., Shi, E., Bai, F., Perrig, A., 2009. TACKing together efficient authentication, revocation, and privacy in VANETs. *In: Proc. of the 6th Annual IEEE comm. society conference on Sensor, Mesh and Ad Hoc Comm. and Networks* (SECON'09). IEEE Press, pp. 484-492.

[9] Stumpf, F., Fischer, L., Eckert, C., 2007. Trust, Security and Privacy in VANETs: A Multilayered Security Architecture for C2C-Communication. *VDI BERICHTE*, pp. 2016-2055.

[10] Wex, P., Breuer, J., Held, A., Leinmuller, A., Delgrossi, L., 2008. Trust issues for vehicular ad hoc networks. *In: Proc. of the 67th IEEE Veh. Tech. Conference* (VTC2008-Spring), Marina Bay, Singapore, pp. 1550-2252.

[11] Papadimitriou, A., Katsaros, D., Manolopoulos, Y. 2010. Social Network Analysis and Its Applications in Wireless Sensor and Vehicular Networks. In: *Lecture Notes of the Inst. for Comp. Sciences, Social Infor. and Telecomm. Engineering,* 2010, 26(10), pp. 411-420.

[12] Lin, X., Lu, R., Zhang, C., Zhu, H., Ho, P.-H., Shen, X. 2008. Security in vehicular ad-hoc networks. *IEEE Communications Magazine*, 46(4), pp. 88-95.

[13] Mishra, B., Nayak, P., Behera, S., Jena, D.. 2011. Security in vehicular adhoc networks: a survey. In *Proc. of the 2011 Int. Conf. on Comm., Computing & Security* (ICCCS '11). ACM, New York, NY, USA, pp. 590-595.

[14] Hong, X., Huang, D., Gerla, M., Cao, Z. 2008. SAT: situation-aware trust architecture for vehicular networks. In *Proc. of the 3rd intl. work. on Mobility in the evolving internet arch.* (MobiArch '08). NY, USA, pp. 31-36.

[15] Car 2 Car Consortium, official web page, last accessed July 07th, 2011, from http://www.car-to-car.org/.

[16] Huang, D., Zhou, Z., Hong, X., and Mario Gerla. 2010. Establishing email-based social network trust for vehicular networks. In *Proceedings of the 7th IEEE conference on Consumer communications and networking conference* (CCNC'10). IEEE Press, Piscataway, NJ, USA, pp. 849-853.