A Security Protocol for Vehicular Distributed Systems

Catalin Gosman[*], Ciprian Dobre[*], Valentin Cristea[*]
[*] University POLITEHNICA of Bucharest, Romania
[*] Bucharest, Romania
E-mails: catalin.gosman@cti.pub.ro, {ciprian.dobre, valentin.cristea}@cs.pub.ro

Abstract— Vehicular Ad-Hoc Networks (VANETs) have the potential to optimize traffic in modern urban areas, reduce congestions and pollution, and increase passenger safety and comfort. Applications designed for such networks pose new security constraints. The mobile devices have limited resources to spare, and the network connectivity is reduced because of the mobility of cars. We present a security protocol designed for VANET environments. It guarantees the content of messages against possible attackers. Because privacy of the passengers must be preserved in VANET, the security protocol is designed not to rely on the drivers' identity. The protocol also proves the time and location when a message was sent. We present evaluation results demonstrating that the protocol is able to correctly handle different security threats.

Keywords- security, VANET, networks, protocol, vehicle

I. INTRODUCTION

Vehicular ad hoc networks (VANETs) have a great potential to improve road safety, traffic congestions, and fuel consumption, as well as increase passenger convenience in vehicles. But because they use an open medium for communication, they are exposed to security threats that influence the reliability of these features. Traditional methods for providing security are not well suited for mobile wireless networks because these are large-scale distributed systems, without centralized control, having a very flexible topology and a transmission area which is limited. Mobile network nodes have also small processing capacities.

Usually authentication and access control are the means to provide security in different systems. But in ad-hoc vehicular networks this is inappropriate because message exchanges are based on wireless communication and the topology of these networks is very flexible and does not permit a centralized control.

In this paper we present a security protocol designed to increase reliability for the messages being exchanged in VANET environments. The protocol introduces both a method to sign the messages without relying on the identity of the cars (thus, it ensures privacy of the cars), and a method to guarantee that a particular message was generated in a particular context (location, time).

The protocol ensures:

a) Data integrity – the protocol ensures that the data is not compromised when it is forwarded from secure car to secure car to final destination due to the message appended signature from a secure traffic lights. Also, the message can be verified with similar ones generated in its immediate geographical neighborhood at a close moment of time (the secure semaphore in the near proximity is a point a trust that emits signatures for vehicles passing by).

b) Data availability – the protocol can cope with attackers trying to make the wireless network unavailable because each message is transmitted on a number of alternative paths. In order to receive its destination, a message can be passed by means of unicast (if the destination is in the transmission range of the source) or broadcast (the message is transmitted to all neighbors in the near proximity, neighbors that will route the message to destination, also, by means of broadcast).

c) Guarantee of place and time for a particular message – every driver can send messages, but once a message is received the protocol guarantees that it was generated in a particular location at a certain moment of time, and not someplace else.

d) Privacy – drivers are not willing to participate in the protocol with their own "identity". No driver is willing to recognize that he was in a particular location participating in a communication, while in reality he was supposed to be somewhere else. The protocol guarantees privacy concerning drivers' identities. It does not reveal the true identity of a driver; instead it uses a random generated ID for secure cars in traffic.

e) Mobility constrains – messages are successfully sent without limiting the mobility of the secure cars. The way messages are transmitted (through broadcast or unicast) does not impose particular routes or speeds for the drivers to follow.

The paper is structured as follows. In Section 2 we present related work. Section 3 presents the protocol for securing communication in VANETs. In Section 4 we present implementation details of the protocol as an extension of a simulator designed for VANETs, and in Section 5 we present experimental results of the protocol. In Section 6 we give conclusions and present future work.

II. RELATED WORK

The problem of securing communications in VANETs was previously explored by various authors in the research literature. However, currently no solution can guarantee that messages exchanged between cars are not modified; moreover, there are no solutions that can link a particular message to a particular time and place and still preserve the privacy of the car's passengers. In Europe, the Car2Car Communication Consortium conducts several researches in the area [1], while in the USA the IEEE P1609 working group has several initiatives in the field.

Blum and Eskandarian [2] propose an architectural model for securing VANETs, particularly designed to handle several types of "intelligent collisions". The solution is based on a PKI virtual infrastructure. However, the solution considers the existence of secure devices available within the road infrastructure. Gerlach [3] analyzes the particularities of security solutions designed for vehicular networks. Hubaux [4] introduces the concepts of privacy and secure positioning in VANETs and presents several solutions designed for solving them. The author also introduces the Electronic License Plates concept. Parno and Perig [5] analyze several attacks that can occur in VANETs. In [11] the authors describe the typical infrastructure of a VANET environment and address several security issues and solutions to them. The use of digital signature in vehicular networks is discussed in [7].

The CARAVAN scheme [8] proposes a solution to let unsecured cars to preserve their privacy and still securely exchange messages. The proposed solutions considers that cars are clustered in groups in which one particular car acts as a leader and forwards all messages further into the network. This solution however poses several problems: messages can be lost, and the solution involves the use of a leader selection algorithm which relies on the cars' identities. A similar approach is presented in [9]. The authors propose a solution based on message aggregation and group communication. The solution considers that data is transmitted between groups rather than between individual cars. The vehicles form clusters, based on their geographical position, and exchange messages only between members of the same group. In each group a leader is elected and is responsible with the propagation of the data to the cars outside the current group.

Stefan Sosoiu and Alex Wolman presented in [6] a solution for securely linking a particular message to one location. The solution, called "location proof", still presents no guarantees that the message cannot be still compromised by malicious attackers.

Another security model is presented in [10]. The authors proposed a hierarchical architecture. The bottom layer consists of nodes responsible for registration. The upper layer is responsible with the evaluation of correctness and also ensures that only nodes having certain verified properties can actively be involved in the communication process. Although the proposed model covers both message integrity and preserves the privacy in VANETs, it cannot guarantee that a message was generated from a particular location. This is an important property for applications where the decision is taken based on the contextual information.

III. THE SECURITY PROTOCOL

Communication between vehicles in a network characterized by high dynamism, geographical positioning, and sporadic connectivity possess unique security issues. The designed protocol aims to address these issues, covering general problems related to security, such as privacy, integrity, availability, non-repudiation. The protocol is modular, scalable, structured in several states.

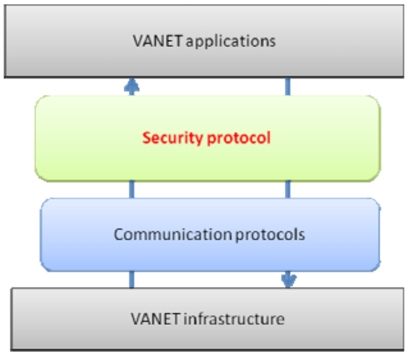


Fig.1. The role of the protocol in a VANET environment.

The security protocol provides secure transmission of messages between entities (vehicle-to-vehicle or vehicle-to-infrastructure communications) in traffic (Figure 1). The protocol is designed and implemented for VANETs, for highly partitioned environments, featuring dynamic connectivity between component nodes of the network. It can assist with security constraints various VANET applications, and it uses the functions provided by existing communication protocols currently used in VANETs.

The description of the protocol is presented in Figure 2. As it is used for securing communication in VANETs, the protocol considers the existence of several entities. Such entities are the *secure car* and the *secure traffic light*. The secure car is a car that can run the security protocol proposed in this paper.

The approach for securing messages transmitted between cars is based on the existence of a certification authority that is presented in the area. In Figure 2, this entity is represented by the secure traffic light. The entity must be available at the road infrastructure level. It can be a traffic light equipped with an access point and connected to a server for example.

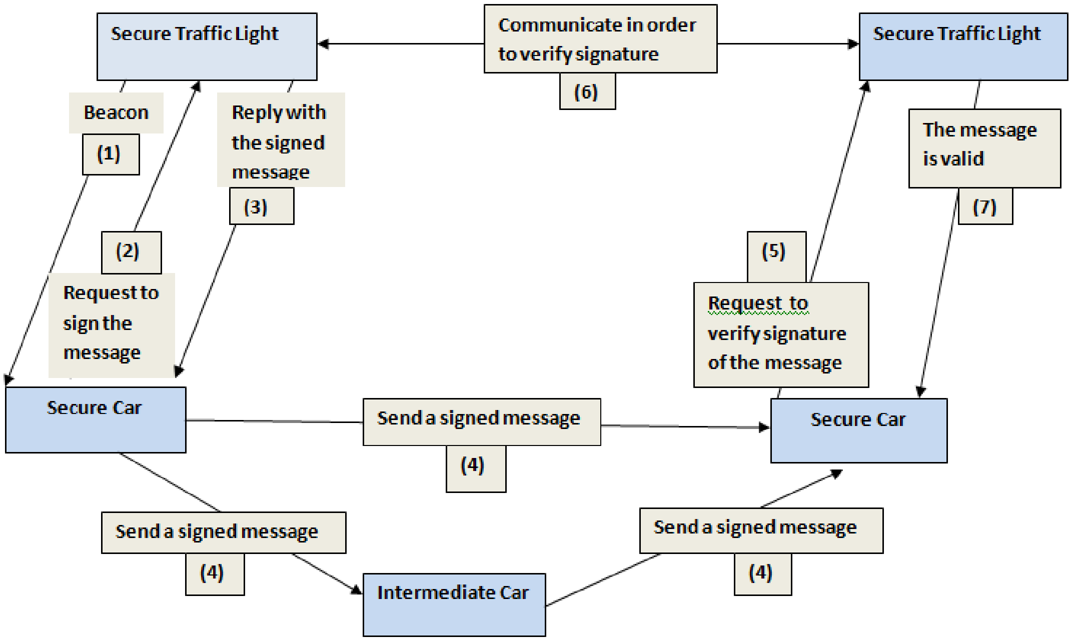


Fig. 2. The security protocol.

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 purpose of the protocol is to provide a solution to secure messages between vehicles in order for the destination secure car to verify the legitimacy of the incoming messages. Secure traffic lights (part of the Infrastructure) act as certifying entities that help secure cars prove the legitimacy of received messages. In the proposed solution, we consider that secure traffic lights can communicate one with each other (for examples, the communication between secure semaphores is possible considering that all secure traffic lights communicate one with each other by means of a separate wired network). Considering that secure traffic lights can communicate one with each other, they can verify the signature of the message using the (public key, private key) pair. If the current secure semaphore can't decide on the legitimacy of a message because it did not sign it, the message will be checked with the other secured points of the infrastructure in order to determine its legitimacy.

The main elements on which the proposed solution is based on are the vehicle location in the moment when it transmits a message, the time at which emission occurs, the existing certification authorities in the area at the start of transmission.

The communication between vehicles starts when a secure car wanting to send a message arrives in the proximity of a secure traffic light. So, in order to initiate communication, a secure car must know about the existence of an entity (a traffic light in this example) which may validate and sign the messages being sent.

In the protocol, when a vehicle wants to send information to another one, it first waits for a beacon from a secure traffic light (or stored messages until a traffic light is found). Traffic lights periodically transmit beacons to all secure cars in their proximity using broadcast messages. Once a beacon is received, the secure car sends the message it wants to transmit to the secure traffic light, where it is signed. When the car received more beacon messages (it is located between multiple semaphores), it considers the first one received and ignores the rest.

Considering the mobility factor specific to VANET networks and the fact that secure cars have restricted broadcast area, the sending of the message to the secure traffic light to be signed is achieved such as:

- if the secure traffic light is in the transmission range of the car, then the message is sent directly to the secure traffic light for signing;
- else, the message is routed through intermediate secure cars to the secure traffic light.

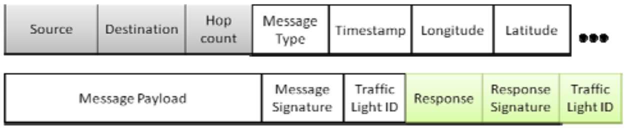
The relevant information contained in the package consists of the timestamp when that message was issued, the current location where the message was issued and the actual message. This information is validated and signed (payload, together with position and timestamp) by the secure traffic light. In practice, for signing the messages, we generate a DSA key pair. When the car receives back from the secure traffic light the message trailed with its signature, it sends the packet to the destination secure car.

The sending of the signed message to the destination is accomplished in several ways:

- if the destination is in the extent of the issuing source, then the message is sent directly;
- else, the message is routed through existing intermediate cars to its final destination.

Once the message reaches its destination, the destination car first validates it. This is accomplished by sending the message further to the nearest secure traffic light. As fixed wired points, traffic lights can also communicate with each, so between them it is easier to verify the signature of a message. Again, sending the message to the nearest secure traffic light is done directly, if the semaphore is in the car's range, or routed through multiple hops (intermediate cars).

Data validation is performed at the level of the secure traffic light, the last entity comparing the digital signature with the fields that help established it. The result of the verification is then sent back to the vehicle which requested this validation. If the answer is positive, the message is further processed, otherwise it is discarded.



Source	Destination	Hop count	Message Type	Timestamp	Longitude	Latitude	●●●

Message Payload	Message Signature	Traffic Light ID	Response	Response Signature	Traffic Light ID

Fig.3. The structure of a message.

The protocol still considers the same message formats used within the traditional VANET communication protocols. In addition, the protocol adds several fields (Figure 3).

The secure traffic light ID field is used to recognize the identity of the fixed entity (traffic light) that signed a particular message. Based on this field, the traffic light from the other end can request a public key and initiate the validation process of a received message. Location and timestamp fields certify that the sender is situated in a particular geographical location and the message was issued at a certain moment of time. Common attacks are based on the fact that users are tempted to lie regarding their geographical position or time when they transmit information. Based on these fields a car can decide to accept or reject a particular message (based on its location proof, for example).

Location is a meta-data certified by a component of the wireless infrastructure (secured traffic lights). To use the positioning mark, an application must trust the infrastructure in order to validate the geographical positioning. For any type of communication, vehicles demand traffic lights to sign their messages. The infrastructure role is only to sign and validate messages for vehicles in its transmission range. Moreover, the protocol allows flexibility because such digitally signed messages can be used in a variety of services.

Messages, regardless of their type, contain the "number of hops" field that prevents further message routing. Also, the designed protocol holds an internal counter calculating the timeout for messages that require such a thing. Timeout mechanisms and maximum number of hops prevent the phenomenon of looping messages indefinitely.

In terms of performance, the protocol supports a very rigorous validation, both at the source and at the destination for each secure message. The protocol ensures validation at source; before a secure car transmits a message to the destination, it checks if the message was not forged using the signature appended at the end of the message. If the signature appended by the secure traffic light corresponds to the appropriate fields that helped forming it, the message is valid and can be transmitted. At destination, the legitimacy of the message is checked up with the help of a secure semaphore in the near proximity.

IV. Implementation Details

The main entities participating in the protocol are the secure car and secure traffic light. During communication, these entities pass through several states, determined by the occurrence of specific events. The transition diagram for the mobile entities (secure cars) is presented in Figure 4. A car is first in the free state. In this state the car did not receive any messages from other road users and did not send any message to other participants.

When the secure car receives a beacon from a traffic light, it moves into the state RECEIVED_BEACON. The secure car can pass into the INTERMEDIATE_CAR state, meaning it is willing to route messages for other vehicles, or into the START_COMMUNICATION state, the moment it receives back from the traffic the digitally signed message. When a secure car receives a message from another car, it passes into the state CAR_RECEIVED_MESSAGE. The message is processed by the destination after receiving the response from the validating traffic light. Sending a message to a secure traffic light for verification can be done directly, if the traffic light is in the transmission area of the car, or routed through other cars, otherwise. As noted, secure cars can always pass to the INTERMEDIATE_CAR state. Once an answer is received from the infrastructure, the secure car goes into the CAR_RECEIVED_ VALIDATION_TRAFFIC_LIGHT state.

In order to create digital signatures, each secure traffic light possesses a pair (public key, private key). The message is signed with the private key, but the verification of the signature is obtained using the public key. Each pair (public key, private key) is specific to a particular traffic light. Figure 4 reveals the independency concerning vehicle's states. The arrows in the diagram are bidirectional, showing that a secure car can go back and forth from a state to another (the reasons why states change are previously described). For example, while a secure car has just received a beacon and is in the BEACON_RECEIVED state, it can also receive a message and change its state to SECURE CAR_RECEIVED_MESSAGE. Still, each of this states are independent and, once a state is reached, specific actions described above are taken.

The secure traffic light is the fixed entity in the protocol. Its role is to sign messages sent by other cars in the vehicular network, and to verify the validity of messages. The possible states and corresponding transitions in this entity's case, according to the proposed protocol, are presented in Figure 5.

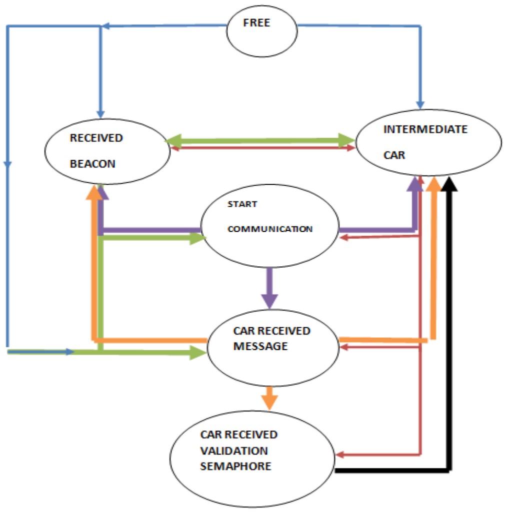


Fig.4. Possible car's states.

The secure traffic light periodically transmits beacons. This initial state is BEACON_SENT. When a validation request message is sent by a secure vehicle the traffic light moves to the CHECKING_MESSAGE state. The state BEACON_SENT and the state CHECKING_MESSAGE do not exclude themselves. The transmission of the beacon is independent of the arrival of messages at the secure traffic light for verification.

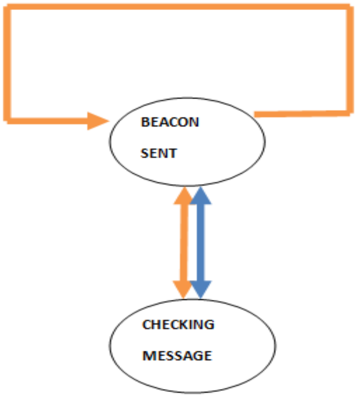


Fig.5. Possible states in case of a fixed entity.

When the semaphore is in the CHECKING_ MESSAGE state, it verifies if a message was not corrupted. In order to accomplish this, it checks the payload, timestamp, longitude and latitude fields of the message against the signature attached to the message. Considering the possibility that a received message was not signed by this particular traffic light, the semaphores must be able to communicate with the rest of the network infrastructure to check its legitimacy.

Figure 5 reveals the independency concerning secure semaphores' states. The arrows in the diagram are bidirectional, showing that a secure traffic light can go back and forth from a state to the other (the reasons why states change are described above). For example, during the time a semaphore is transmitting a beacon, it can also receive a message to sign or to validate.

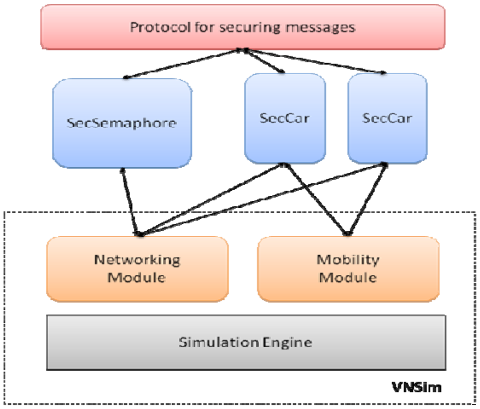


Fig.6. The components implementing the protocol.

Starting from the description of the protocol, we evaluated its behavior in a simulated environment. We were particularly interested whether it is capable of coping with a wide range of possible attacks and how it affects the performance of the underlying VANET environment. For that we extended the VNSim simulator [12], a generic VANET traffic simulator that uses both the microscopic and macroscopic models in order to accurately evaluate the performance of a wide range of VANET technologies. On top of the model already provided, we added the components and mechanisms previously described (Figure 6).

V. Experimental Results

To evaluate the proposed security protocol we executed several simulation experiments: forge the message at intermediate secure cars before reaching a semaphore in order to be signed, forge the message at source before transmitting it to the destination, forge a message so that it does not have a signature appended to its end, DoS attacks targeted on a specific secure cars that receives forged messages from numerous attackers, vehicles that are in the INTERMEDIATE_SECURE CAR state and stop forwarding messages. These experiments considered a mobility scenario that resembles the vehicular traffic in the campus of the University POLITEHNICA of Bucharest (Figure 7). The scenario consists of 16 secured semaphores and variable flows of cars (an average of 50 cars/ lane/hour). We were interested in the capability of the protocol to solve a number of attacks and the overhead introduced by its use.

For example, in case of the secured semaphore, we were interested in its capability to correctly recognize altered messages (i.e that were possible modified by cars acting as intermediate routing nodes) or whether it is capable to handle a larger number of secure cars.

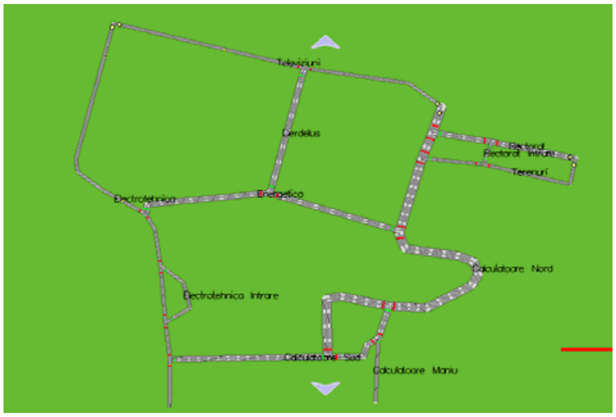


Fig.7. The scenario map used in the simulation experiments.

We evaluated how the protocol behaves in a scenario where a number of attackers try to modify the content of forwarded messages. In this case attackers forward signed data to its destinations, but they willingly change the payload of the received messages. This happens, for example, when an attacker wants to influence the dissemination of certain information. In the scenario the number of attackers corresponds to a normal distribution having an average of 35% of the total number of cars.

The results in Figure 8 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 behavior (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.

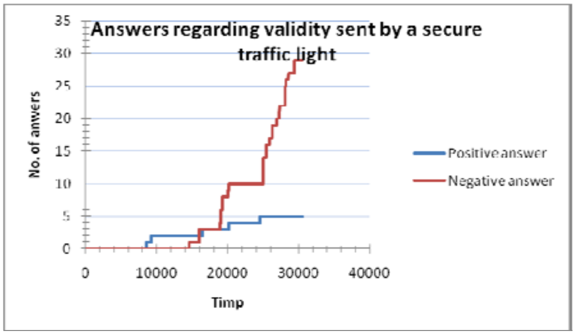


Fig.8. Answers concerning validity sent by the secure traffic light.

The results in Figure 9 correspond to the variation in time of the number of connections established between secure cars. A connection consists in the transmission and proper reception of a message between source and destination. We can see that the graphic has an ascending slope due to the fact that forged messages receive negative validation at destination (the legitimacy of the message at destination is obtained by means of interrogating a secure traffic light regarding the received message). In this case the semaphores recognize the compromised messages and inform the secure car.

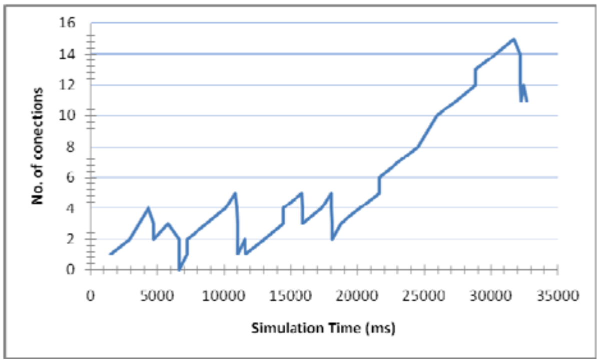


Fig.9. The number of connections established between cars.

We also evaluated how the protocol handles the situation when messages are sent to be signed by the semaphore, but in between attackers modify the message. The semaphore signs the modified message, not knowing about the attack. However, when the message is received back by the source car, the modification is correctly discovered.

Another set of experiments evaluated how the protocol handles attackers modifying the signed message being sent for verification from the destination car to a secure semaphore. The protocol still leads to the correct identification of the problem.

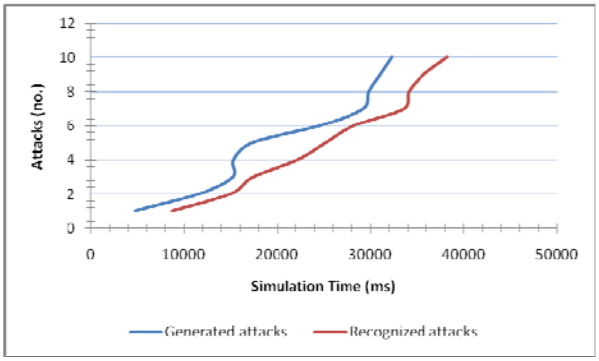


Fig.10. Attacks correctly stopped in the experiment.

Another attack that presents interest in VANET is Denial of Service (Dos). The protocol withstands this attack due to its implementation design, but also due to the fact that a secure car can impose a limit on the number of messages that can be processed at a certain moment of time. If the limit is exceeded, all the messages that exceed the limit are discarded until the secure car can process a part of the previous messages in order for other new messages to be received.

For all attacks mentioned not only the protocol correctly handles the threats, but also the performance of the VANET environment (throughput in the wireless network, processing capability of the secure cars, etc) is not affected beyond rendering it impossible to be used anymore. The overhead imposed on the network throughput is caused by appending to a message a digital signature in order to be able to validate it. Based on the experiments proposed, we have discovered that the overhead is around 28% for the considered scenarios. Also, the transmission needs extra time because of the secure car-to- secure traffic light communication; this overhead puts an extra 29% to the regular time of transmission between two secure vehicles when using the protocol. These costs should be, however, put in balance with the security benefits brought by the usage of the protocol.

VI. CONCLUSIONS

Vehicular ad hoc networks (VANETs) have great potential to improve road safety, traffic congestions, and fuel consumption, as well as increase passenger convenience in vehicles. But because they use an open medium for communication, they are exposed to security threats that influence the reliability of these features. We propose a protocol designed for securing communication in such environments.

The security protocol considers the particular characteristics of VANETs. It ensures data integrity, reliability, non-repudiation, preserves privacy and links a message to a particular time and place the message was generated.

The security protocol was implemented in a VANET simulator and we presented evaluation results of its capability to handle a wide range of attacks that are characteristics to such environments. We demonstrated that the protocol is robust and can handle various security threats. In addition, the protocol induces little performance loss on the vehicular infrastructure.

In the future we plan to further extend the research and consider various other alternatives of signing and validating messages in VANETs. We also plan to extend the protocol by also considering the semantics of the messages and using various trust-computation protocols.

VII. ACKNOWLEDGMENTS

This work was supported by CNCSIS-UEFISCSU, project "TRANSYS – Models and Techniques for Traffic Optimizing in Urban Environments", number PN II-RU code/2010, "CNCSIS-PD" ID: 238.

VIII. REFERENCES

[1] CAR-2-CAR project, official web-page, last accessed July 1st, 2010, from http://www.car-2-car.org/.

[2] Blum, J., A. Eskandarian, "The threat of intelligent collisions", *IT Professional* **6**(1), pp 24–29, 2004.

[3] Gerlach, M., "*VaneSe – An approach to VANET security*", in Proc. of V2VCOM'05, San Diego, California, USA, 2005.

[4] Hubaux, J.-P., S. Capkun, J. Luo, "The security and privacy of smart vehicles", *IEEE Security and Privacy Magazine* **2**(3), pp. 49–55, 2004.

[5] Parno, B., A. Perrig, "*Challenges in securing vehicular networks*", in Proc. of the Workshop on Hot Topics in Networks (HotNets-IV), College Park, Maryland, USA, 2005.

[6] Saroiu, S., A. Wolman, "*Enabling New Mobile Applications with Location Proofs*", in Proc. of the 10th workshop on Mobile Computing Systems and Applications, Santa Cruz, California, USA, 2009.

[7] Gollan, L., C. Meinel, "*Digital signatures for automobiles*", in Proc. of Systemics, Cybernetics and Informatics (SCI), Orlando, Florida, USA, 2002.

[8] Sampigethaya, K., L. Huang, M. Li, R. Poovendran, K. Matsuura, K. Sezaki, "*CARAVAN: providing location privacy for VANET*", in Proc. of the Workshop on Embedded Security in Cars(escar), Springer Monograph Series, 2005.

[9] Raya, M., A. Aziz, J.-P. Hubaux, "*Efficient secure aggregation in VANETs*", in Proc. of the Third ACM International Workshop on Vehicular Ad Hoc Networks (VANET'06), Los Angeles, California, USA, 2006.

[10] Gerlach, M., A. Festag, T. Leinmuller, G. Goldacker,C. Harsch, "*Security Architecture for Vehicular Communication*", in Proc. of the Fourth International Workshop on Intelligent Transportation , WIT Hamburg, Germany, 2007.

[11] Raya, M., Hubaux, J., "*The security of vehicular ad hoc networks*", In Proc. of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, Alexandria, VA, USA, November 2005.

[12] A. Gainaru, C. Dobre, V. Cristea, "*A Realistic Mobility Model based on Social Networks for the Simulation of VANETs*", In Proc. of the VTC-Spring 2009 Conference, Barcelona, Spain, 2009.

.