Journal of Universal Computer Science, vol. 18, no. 6 (2012), 857-873
submitted: 15/10/11, accepted: 15/2/12, appeared: 28/3/12

Countermeasures to Prevent Misbehaviour in VANETs

Jezabel Molina-Gil, Pino Caballero-Gil, Cándido Caballero-Gil
(University of La Laguna, Tenerife, Spain
jmmolina@ull.es, pcaballe@ull.es, ccabgil@ull.es)

Abstract: A key aspect to ensure that Vehicular Ad-hoc NETworks (VANETS) work properly is the provision of reliable and real time information to users. In order to achieve this goal, on the one hand, nodes must cooperate actively in relaying the messages to reach as many users as possible to warn them about possible hazards. On the other hand, users should be able to rely on the received information, so they should be able to verify that the relayed network data are true. As distributed and decentralized networks, security problems such as prevention of false information injection, and detection of misbehaviour could be solved through cooperation among nodes. In this work we propose a set of countermeasures to prevent selfish behaviour and malicious attacks, making use of node revocation through cooperation enforcement mechanisms and isolation of malicious nodes from the network. The proper performance of the proposed techniques has been evaluated with many simulations, and the results show that the countermeasures described in this work increase not only efficiency but also security of communications.

Key Words: VANETs, cooperation, self-management, security, misbehaviour, ITS
Category: SD C.2.0, C.2.1, C.2.2, C.2.3, C.2.4

1 Introduction

Vehicular Ad-hoc NETworks (VANETs) are generally defined as Mobile Ad-hoc NETworks (MANETs) formed by vehicles. Their main goal is to provide information to drivers so that their deployment allow enhancing safety, efficiency and comfort in road travel. In these networks, warning messages affect drivers' decisions, so any incorrect message could lead to increase several important parameters such as the time required to reach the destination, fuel consumption, environmental pollution and, in the worst case scenario, traffic accidents.

VANETs, as smart technologies in Intelligent Transportation Systems (ITS), have become a hot topic in network research. In the near future, such networks will reduce the number of deaths from traffic accidents, by providing real time information about traffic and road status. In addition, VANETs might be used for other practical applications such as finding parking spaces, for example.

Research on ad-hoc networks raised the need for enhancing cooperation between nodes as a prerequisite for their proper operation. VANETs, as an evolution of these networks, also have need for cooperation. However, due to characteristics such as high mobility, real-time constraints, scalability, gradual deployment and privacy, VANETs present additional challenges. A key aspect for the proper functioning of the network is to provide reliable and real-time information about traffic and road conditions. To achieve this goal, nodes must actively cooperate in sending received event warnings to the nodes they find during their life on the network. It is possible that malicious users try to get benefit from the information provided by the network and at the same time minimize their battery consumption and storage space, by configuring their devices to receive information from the network but without cooperating in relaying it. Therefore, the existence of some mechanisms to prevent these nodes affect the network performance is necessary.

There are many situations where communication among vehicles and cooperation in the relaying of packets can help to prevent accidents and to avoid collapses. Nevertheless, the behaviour of selfish nodes could break the network into pieces causing a passive Denial of Service (DoS). It is rational to assume that each node has the target of maximizing its own benefit by taking advantage of the network services while minimizing its own contribution to the network. Therefore, the need to motivate nodes to relay information for the benefit of other nodes is justified.

This work proposes the use of cooperative tools that can be implemented with current technology, such as laptops, smartphones, etc., provided with Global Positioning System (GPS) equipment and wireless networking communication. The goal of this work is to create a vehicular ad-hoc network using these technologies inside cars so that they can be also used as an emulation of the devices that will be implemented in future cars to form VANETs. Hence, real data obtained from these networks will be useful for the analysis of the operations in future VANETs.

Nowadays, there are several GPS software applications that provide drivers with information about traffic conditions compiled by local traffic authorities, police departments or other centralized systems. However, in most cases the information provided to drivers is not in real time because it does not reflect events that have just produced and/or involves lack of user privacy due to the centralized operation. In addition, most software tools that provide this service, such as Google Traffic application, require 3G connection, which represents an additional cost for users. Therefore, the motivation to study the secure and efficient deployment of new self-organized and cooperative proposal of VANET deployment, instead of the existing GPS software applications is clear.

This paper introduces a mechanism to provide real and reliable information to those vehicles that are actively involved in the correct operation of the network. The scheme includes a decentralized system for the revocation of selfish and malicious nodes, using cooperation among nodes and isolation of attackers, based on the use of reputation lists and rewarding mechanisms.

This paper is organized as follows. Several works related with cooperation in VANETs are summarized in Section 2. Some cryptographic preliminaries and the background of the scheme are respectively described in Sections 3 and 4. The proposed approach is introduced in Section 5, where specific definition of some tools for the detection of false information provision and non-cooperation are given. Section 6 provides a detailed description of the proposed system to isolate misbehaving nodes. Sections 7 and 8 include the analysis of the proposal from the points of view of robustness and performance. Finally, conclusions are included in Section 9.

2 Related Work

In order to develop VANETs to their full potential, some schemes to stimulate cooperation in transmitting and forwarding packets need to be developed according to the specific properties and potential applications of VANETs. Indeed, cooperation enforcement has been a hot research topic in MANETs. Buttyan and Hubaux proposed in [Buttyan and Hubaux 2003] and [Buttyan et al. 2007] the use of virtual credit in incentive schemes to stimulate packet forwarding in MANETs. Also, cooperation in MANETS was studied in [Ben Salem et al. 2006] where the assumption that each node has the goal to maximize its own benefit by enjoying network services and at the same time minimizing its contribution was presented. There it was proposed to encourage nodes to relay information for the benefit of other nodes through a charging and rewarding scheme. However, solutions in MANETs are not directly applicable to VANETs mainly due to their high mobility, limited connectivity and large scale. Thus, Li et al. discussed some unique characteristics of incentive schemes for VANETs in [Li and Wu 2008] and proposed a receipt-based rewarding scheme that focuses on the incentive for broadcasting. However, the proposed scheme for receipt counting has an overspending problem. Based on the specific characteristics of VANETs, a more comprehensive weighted method for rewarding was proposed in [Hernández-Goya et al. 2009]. Anyway, most existing solutions based exclusively on rewarding mechanisms suffer from lack of fairness assurance and reliance on costly tamper-proof hardware or on trusted third parties. These problems are not present in the proposal of this work.

Malicious attackers can cause the VANET to be broken into pieces so that the network cannot provide services such as route establishment and packet forwarding to legitimate users. In this sense, the behaviour of selfish nodes can cause a passive DoS. [Isaac et al. 2010] discusses some of the main security threats and attacks that can be exploited in VANETs. Similarly, [Mousannif et al. 2011] uses routing for communications, and introduces cooperation as a service, based on a cluster structure. Both papers are mainly focused on the design of routing schemes, unlike the present proposal.

Several authors have proposed combined approaches to the topic of cooperation in VANETs. The proposal called VARS, described in [Dotzer et al. 2005], uses direct and indirect trust as well as appended opinions to enable confident decisions on event packets. The main problem of such a proposal is that it involves accumulation of reputation evaluation over much time. [Fonseca and Festag 2006] gives an overview of existing approaches that try to provide routing security to conventional MANETs and analyses whether these approaches can be applied to secure VANETs. To promote cooperation among nodes and to protect VANET packets during propagation, [Wang and Chigan a2007] proposes a dynamic trust-token based cooperation enhancement mechanism. Another interesting reputation system was described in [Wang and Chigan b2007], where trust relationships and packet-acceptance decisions are based on instant observation and relaying data about node behaviour. However, both watchdog schemes have some drawbacks, implying that tampered packets may be propagated.

[Xiong et al. 2010] proposes a flocking scheme for groups of vehicles, which focuses on their decentralized coordination so that they can cooperate in complex environments. A good example of VANET application that requires cooperation is described in [Lee et al. 2007], which proposes a framework for commercial ad dissemination in VANETs where vehicles receive an incentive for forwarding and carrying advertisements. Unlike the above papers based on rewarding mechanisms, several recent reputation schemes have been proposed based on node behaviour with respect to its collaborative operation monitored by other nodes. [Lo and Tsai 2009] used an event-based system to prevent nodes from spreading false traffic messages through the determination of whether incoming traffic messages are significant and trustworthy to the driver. [Schmidt et al. 2008] described a mechanism for detecting possible malicious nodes through the use of three different modules whose sum up determines node reputation.

However, all the aforementioned tools, including the reputation system proposed in [Raya et al. 2007], require Certification Authorities (CAs) responsible for delivering keys and certificates. In particular, [Sun and Fang 2008] proposed that such a role be played by a regional transportation authority, which can be a state, province, etc., while other authors proposed a Department of Motor Vehicles [Li and Wu 2009]. Therefore, none of those solutions can be considered applicable to the fully distributed and decentralized networks discussed in this work, where several countermeasures combining rewarding and reputation ideas are proposed.

3 Cryptographic Preliminaries

Important research issues of VANETs are the cryptographic needs of these networks, such as authentication, data integrity, privacy and confidentiality. In order to meet all these requirements, the uses of various known mechanisms such as public-key digital signatures and pseudonyms have been included in the proposed scheme.

During the network construction, each user must get a public/private key pair in a decentralized way. In order to achieve this goal, each new node will perform a key exchange with one or more reliable nodes in the network. Additionally, a pseudonym will be given to each new node in order to link it with its cooperative or selfish behaviour, but without revealing its identity. This alias will be created by an automatic generator from its public key, what prevents both the existence of two identical pseudonyms as well as the possibility of generating a false pseudonym to masquerade as another vehicle.

Furthermore, each network node has a key store that contains other nodes' public keys signed by reliable users of the network. When two nodes meet and want to communicate with each other, their public keys are exchanged. Each public key will be looked up at the key store, and if there is no coincidence, both nodes exchange their stores. Thus, both nodes try to find a common path in the resulting web of trust [Hubaux et al. 2001]. Otherwise, nodes cannot authenticate and trust each other. It is possible that the probability of coincidence at the beginning of the network is small, so lower security levels have to be defined then. When the network reaches a sufficient size, taking into account the small world experiment [Milgram 1967], these levels may be raised. The experiments associated with the so-called "six degrees of separation" [Newman et al. 2006] are based on the idea that if a person is one step away from each person it knows and two steps away from each person who is known by one of the people it knows, then everyone is at most six steps away from any other person on Earth. This idea is used in our work in an important aspect because according to the principle of "six degrees of separation", the probability to find a common chain between any two key stores is high. Besides, mobility, one of the important characteristics of VANETs, allows to efficiently reduce uncertainty and to speed up trust convergence.

4 Overview of the Proposal

The main aim of this work is to prevent a bad behaviour that could endanger the network connectivity and its proper functionality.

On the one hand, we present a mechanism capable of automatically detecting malicious nodes that try to transmit false information about the existence of an event. For this purpose, we present a tool that allows determining this kind of attack through the cooperation of neighbouring nodes and prevents such attackers from getting benefit from the information relayed within the network.

On the other hand, this paper proposes a mechanism that encourages nodes to participate in packet retransmission, and isolates nodes that do not cooperate in packet relaying.

The first mechanism for false information detection is based on reputation schemes whereas the second mechanism for non-cooperation detection uses the rewarding paradigm.

As shown above, both the detection of events and packet retransmission present the possibility of attacks. In both cases, the solution is to detect and isolate malicious nodes from the network. For this purpose, we use cryptographic security tools that allow us to guarantee authenticity of information, privacy of users and non-repudiation on generated information. Thus, digital signature schemes are used to link author and content of each sent message and, like in [Buttyan et al. 2007], pseudonyms are used to avoid disclosing real identities of nodes.

The following summarizes the operation of our proposal. For example, if a node detects a traffic congestion, it must notify its neighbours about it so that such communication provides them an augmented reality of what is happening on the road. In this way, other users outside the congestion zone can make decisions in time to avoid possible accidents and traffic jams, for example by finding an alternative route. Neighbouring nodes that can check such event information are responsible for determining the authenticity of the messages, reporting detected forgeries if they exist. Since then fake nodes will not be authenticated by other nodes and will be unable to get any profit from the network. The whole process is automatic and transparent to the network user so that there is a module responsible for detecting false or altered information and informing the network about it. To do it with security, all forwarding messages must be signed by the origin in order to enable nodes to determine which is the node that presents a bad behaviour.

When developing the proposed mechanism, an important problem that was taken into account to make it possible that the system works properly was the requirement that users cooperate by relaying packets to their neighbouring nodes. Therefore, the possibility that legitimate nodes act passively only receiving information from the network is prevented with the proposal. This attack would damage the network passively, by degrading its performance and threatening the connectivity. Consequently, a specific module to determine whether nodes cooperate in the network is included in the proposal. There exists another possible attack consisting in relaying packets to overload the network. In this case, legitimate nodes would actively cooperate in the attack by contributing to disseminate information that is useless or repeated. Tools to avoid this specific type of attacks are also detailed below.

5 Detecting Misbehaviour

The basic idea of this work is that VANETs will allow detecting traffic jams and other events on the road through the automatic exchange among nodes of reports and warning messages about them. This will be done thanks to the information provided by GPS because with GPS software it is possible to know the speed at which nodes are moving and the maximum speed allowed in each lane of the road. Given this information, if a vehicle is travelling at a speed below the minimum, it is probably due to that there is traffic congestion on that road. In this case, a packet will be automatically generated to warn users about the traffic problem. Wireless network technologies allow devices to move freely, what implies that this mobility can affect permanent access to the network. However, in the present proposal this type of permanent connections is not necessary because nodes exchange information when they meet so mobility is not a drawback but an advantage. This design is based on the so-called store-and-forward routing model. In a typical packet forwarding process in VANETs, vehicles meet one another at different times, and packets are opportunistically forwarded. If an intermediate vehicle stores a packet for a long time and actively broadcasts the packet to other vehicles, the packet will be more likely to reach a greater number of vehicles.

In this work we consider that a bad behaviour of a vehicle within the self-managed vehicular network can consist on:

- Inserting in the network false packets with spoofed content on the state of the road or inserting many times the same packet to try to launch a DoS attack.
- Not cooperating in relaying packets of its neighbour nodes so that it benefits from the network without cooperating in its operation.

The detection of an attack attempt should be automatic and transparent to the user. Hence, in order to achieve it, the proposed system uses environmental parameters and compares them with parameters of the received packet. Thus, all data packets in our proposal contain at least the following information:

- **GPS coordinates.** The GPS coordinates will help in two ways. On the one hand, combined with the movement direction, they will provide information about the place where an event data packet was originally generated and where the problem is located. On the other hand, they will allow discarding event warnings beyond a certain range because in most cases, information generated at a certain location in a VANET is not interesting out of a radius distance. Thus, for instance, an event data packet can be generated in coordinates (X,Y) and certain range of interest for this packet can be defined within a radius R. In this way, that packet will not be broadcast when it reaches R. The particular size of the radio R must be fixed by the source node according to the type of road and the type of event warning.

- **Speed.** A parameter that the GPS device uses to detect the fastest or shortest route to the destination is the maximum limit of all speeds in the used via. In this sense, our system can detect whether there is a traffic jam in a specific highway through the speeds at which vehicles move on it. With this information, the GPS device will be able to make calculations to determine if going through the traffic jam will take less time than modifying the route. Otherwise, it may propose a new way to reach the destination in the shortest time possible.
- **Next via.** Information about the next via allows knowing whether a traffic jam occupies the entire highway or only a given lane of the highway.
- **Timestamp.** The parameter that gives the time at which the packet was sent allows determining whether the received information is new or old. This makes possible to have updated information about the road all the time.

5.1 False Information Detection

The next paragraphs explain how the aforementioned information contained in data packets can be used to detect attempts of false information retransmission:

- **GPS coordinates:** If a vehicle A gives information about dense traffic in a road where another vehicle B is driving at an appropriate speed, the vehicle B can report that A is introducing false information. Moreover, if a vehicle is sending an event data packet outside the fixed radius R, this can be reported as a DoS attempt.
- **Speed and next via:** If a vehicle sends information about a traffic jam in the same geographic coordinates where another vehicle is circulating at a high speed, this should be reported as a fraud. Indeed, specific cases such as when the next via in its route is nearby, should be dealt as an exception for detecting a traffic jam warning.
- **Timestamp:** If a vehicle is transmitting information with an expired Timestamp, this is considered as a DoS attempt.

5.2 Non-Cooperation Detection

A vital aspect for the operation of the network is to provide real-time and trustful information to others nodes. This is achieved through node cooperation in relaying packets to their neighbouring nodes. In this work we identify cooperation of nodes through time-stamped ACKnowledgment (ACK) packets.

In particular, if a node A receives or produces some event data packet, before providing it to another node B, it asks B about B's cooperation in the network. The node B answers A by providing it with the last ACK it has received. If the timestamp included in such ACK exceeds the threshold T defined by the protocol depending on the network size, the node A does not send the packet to B. Thus, nodes are motivated to cooperate to upgrade their ACKs.

In order to get the ACK after a retransmission and to avoid selfish behaviour, the system follows the process detailed in Figure 1, where node A, who wants to send the data packet M to B, splits it into two parts (M_1, M_2) in order to ensure that node A receives at least one ACK as proof of its cooperation before B receives the complete packet. When B receives the first part M_1 of the packet encrypted with its public-key $E_B(M_1)$, it sends an acknowledgment signed with its private key and encrypted with A's private-key, $E_A(D_B(ACK_1))$. Then, A sends to B the second encrypted part of the packet $E_B(M_2)$ so that B can recover the full content of the data packet. Finally, B sends a second signed and encrypted acknowledgment $E_A(D_B(ACK_2))$ to node A. It is possible that after receiving the first acknowledgment, A does not send M_2. Also, B might not send the second acknowledgment. In any of these cases, the fraud must be reported through the reputation mechanism based on reputation list described below.

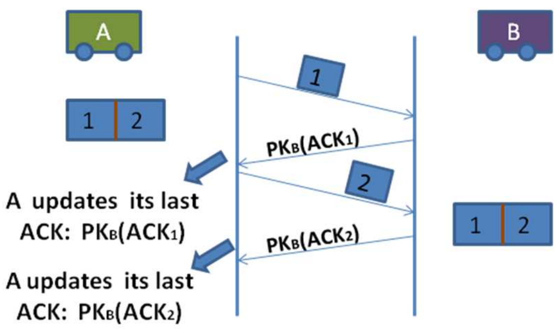

Figure 1: Sending packets and receipt confirmations.

6 Malicious Node Isolation

Each network node maintains two reputation lists, one providing an overview of all malicious network nodes and the other providing the vision about own experience with malicious nodes during its life in the network. The purpose of these lists is to exclude misbehaving nodes from the network, so that nodes are

Table 1: Fields of the GRL.

Selfish node's pseudonym	Misbehaviour Timestamp	Complainant's Signature	GPS Coordinates (X,Y)

motivated to contribute to the network operation in order not to be isolated from it.

Each vehicle stores a list called General Reputation List (GRL) containing revoked pseudonyms corresponding to vehicles that have bad behaviour against the operation of the network. In the absence of a CA, the GRL must be updated through the exchange of the GRLs among neighbouring nodes. Such an update is done each time two cooperative and authenticated neighbour nodes starts a communication. If a vehicle A has an event data packet and meets another node B that is in its GRL, A does not provide B with such a packet. Thanks to this procedure, nodes will not have selfish behaviour within the network. Moreover, if a node A receives a packet from a node who is in A's GRL, A will discard B's packet so that the misbehaving node B will not be able to continue attacking the network. In order to update this list, it is important that the process is efficient and based on a fast search algorithm. Table 1 shows four possible fields in this list. Each record in this list will contain the misbehaving vehicles' pseudonyms. The timestamp of a bad behaviour is used to keep the list updated by deleting old records. Another field including the signature of the node that presented the complaint is also stored. Furthermore, the GPS coordinates field corresponding to the misbehaviour location is included so that they can be used to simplify the GRL if it grows too much.

As previously discussed, a vital aspect for the operation of the network is that nodes cooperate in relaying packets of their neighbouring nodes. To meet this need, we propose the use of the so-called Individual Reputation List (IRL). It allows the node to store information about cooperation got from the different nodes it meets during its life on the network. This list is maintained by each node to store information about its direct own experience with other nodes of the network, so it is totally reliable for the node. Hence, thanks to the IRL the node can make clear decisions on whether to cooperate or not with other nodes. The information in IRL is directly added to the GRL during GRL's exchange.

From the stored GRL, each node can compute a misbehaviour rating r_j for each other node j corresponding to the number of stored complaints from different complainants against j. Thus, the higher misbehaviour rating the lesser probability to send/accept data packets to/from j. In particular, such a probability $prob_j = 0$ if $j \in$ IRL. Otherwise, $prob_j = 1/r_j, \forall r_j \geq 1$, and $prob_j = 1$ if $r_j = 0$.

The IRL is updated whenever the node detects misbehaviour of a vehicle that tries either to forge a message that does not correspond to its real environment information or not to cooperate in the aforementioned retransmission acknowledgment process.

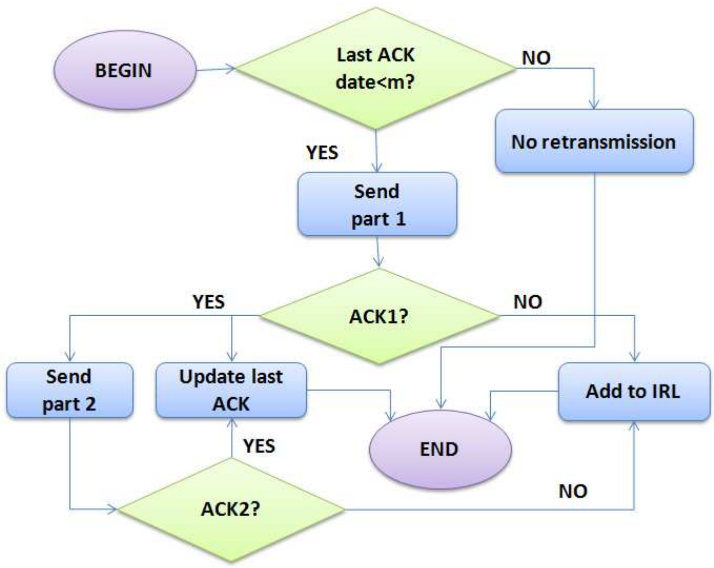

Figure 2: Sender A's Flowchart.

During the aforementioned exchange of packets and acknowledgments, if some node decides not to relay all necessary packets, it is introduced in the IRL of the other node. This would happen if for example A does not send the second part of the packet after B has sent the first acknowledgment, or if B does not send some of the corresponding acknowledgments. Figure 2 shows the flowchart corresponding to the procedure when a node A sends a data packet to a node B, while Figure 3 shows the flowchart corresponding to the process when a node B receives a data packet from a node A.

7 Robustness Analysis

A correct mechanism for cooperation detection must have two characteristics: flexibility and robustness. With regard to flexibility, note that a hardware malfunction can make the device sends messages with an incorrect or expired timestamp. Therefore we should not be too strict and allow nodes to recover from that problem. Moreover, it would be unfair to prevent the access of misbehaving

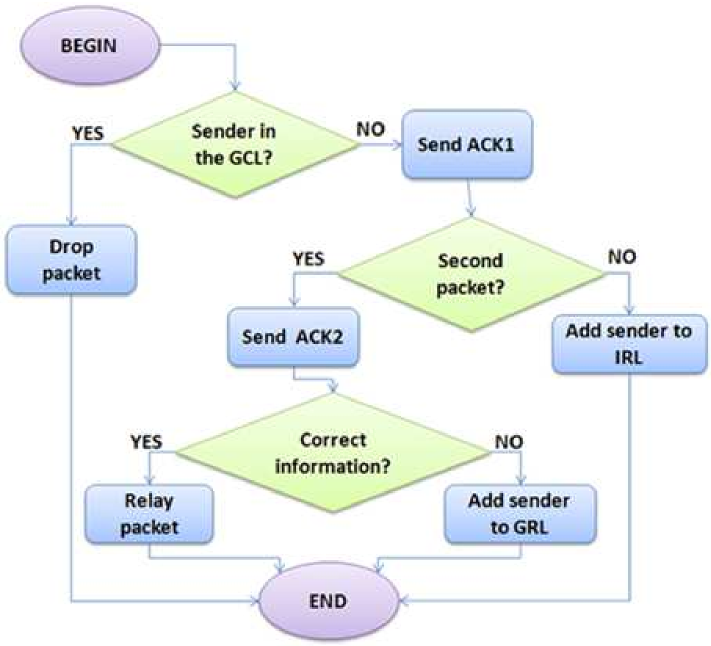

Figure 3: Receiver B's Flowchart.

nodes to the network forever after only one bad behaviour. In order to solve this problem, any node with a reported misbehaviour has two possibilities:

1. To get a new key pair and a pseudonym from a legitimate node belonging to the network. When a node has been marked as an attacker, it will be isolated from the network and will not receive any traffic information. In case of malfunction, the node can request a new key pair from a legitimate network node. Before the node receives it, it must explain the situation to the legitimate node that will provide it with the new key pair if it thinks it is appropriate doing it.

2. In order to wait till records in nodes lists are old enough to be deleted. Once the threshold T is reached, the complaint expires and the node is removed from the lists so that the node is able to re-join the network with its credentials.

The robustness of the proposed mechanism ensures that the information that reaches any node is true, what prevents that nodes can impersonate other nodes by sending fake packets on their behalf. To ensure this, each intermediate vehicle must be able to determine whether the information generated by the source node has not been altered. In this case, the source node signs the packets with its private key. Thus, if the information is altered, the received node will be able to detect it. Furthermore, thanks to these detection mechanisms, selfish nodes can be isolated from the network, what ensures that the nodes involved in the network and the information they send are reliable.

During the security analysis of the proposed protocol, we realized that there exists the possibility of incorrect false information detections. Thus, for instance, there could happen that a vehicle has detected a traffic jam in a road where another vehicle is travelling at an appropriate speed. This could be a common situation where the left lane works properly but there is a traffic jam in a deceleration lane on the right corresponding for example to an exit to a city. In this case, besides the GPS coordinates and movement direction, the lanes have to be determined.

As discussed in the previous section, cooperative authenticated neighbour nodes exchange their GRLs. This implies that a node can try to attack other nodes by inserting false records in their lists. This is the reason why the criterion for determining whether a node must be isolated or not depends on its misbehaviour rating according to the GRLs. On the one hand, if a high number of nodes agree that a particular node is selfish, then it is probably true and consequently the reported node is isolated. On the other hand, if the GRL grows too much, an additional parameter that could be taken into account is the GPS coordinate (X,Y) so that at least two complaints against the same node should correspond to different coordinates (X,Y) to be considered in the GRL.

An unusual situation appears when a vehicle is stopped on the roadway due to an accident, car malfunction or phone conversation for instance. In any of those situations, the automatic mechanism detects a vehicle at 0 km/h on a road and sends a warning about a traffic jam that does not exist. A drastic option to solve this problem would be to revoke the vehicle, which then should ask for a new key pair after explaining what has happened.

Another analysed problem comes from the use of ACK as a cooperative enforcement mechanism. New nodes that have not participated in any packet retransmission have no ACK to receive packets from the network. The simplest solution would be that the authenticator node gives an ACK to them. Another option would be to wait till the new nodes generate own data packets, so that after sharing them with other vehicles, they get an ACK and are able to participate in the network.

The best practical solutions to all aforementioned special situations will be determined during the practical implementation of the proposal.

8 Performance Analysis

Both the feasibility and effectiveness of the proposal have been tested through several simulations. In particular, we used NS-2 and SUMO taking as starting point the simulations analysed in [CaballeroGil et al. 2007]. We simulated the proposed scheme based on a combination of ACK-based rewards and reputation lists in a random environment to see its effects on network and cooperation performance. In order to make a performance analysis of the proposal, several VANET simulations were implemented. This section presents some details and results of these simulations. The aim of our proposal is to determine and isolate from the network all malicious nodes. An interesting analysed parameter is the time required for all network nodes to know which nodes are malicious in order to isolate them and prevent communications with them. The first simulation consists of a network of 100 nodes that make communications between them in a totally random way. Each simulation was performed 100 times for different percentages of malicious nodes. If a node meets for the first time a malicious node, it includes it in its IRL and GRL. If it meets a malicious node that is already in its IRL, the connection is stopped. Otherwise, if the neighbour j is in the GRL, then according to $Prob_j$, it can either stop the communication or continue with it. Both in this last case, and if it connects to a node that is not malicious, make an ACK-based exchange of their GRLs. Figure 4 shows the average time (in min) required for all the simulated networks with different percentages of malicious nodes until all nodes determine who are the malicious nodes. As we can seen, as the number of malicious nodes increases, the time to detect them decreases. This is because there is a greater probability of encountering a malicious node and therefore the number of complaints on those nodes increases. Therefore, the mechanism works faster to isolate malicious nodes when the number of malicious nodes is greater.

Figure 4 shows that where more time is needed by the method is in networks with 15 to 20 per cent of malicious nodes so we took this value and varied the number of nodes in the network from 100 to 1000 nodes to determine how the number of nodes influence in the time needed to isolate malicious nodes from the network. In this case the average warning times (in min) for 100 simulations performed for each different network sizes are shown in Figure 5. As we can see, the time to alert all nodes increases with the increase of the network size. However, the results show that it is possible to isolate the malicious nodes in a reasonable time and independently of the network size because the growth is linear rather than exponential.

Therefore, for all the implemented simulations we can conclude that the proposed cooperative system using reputation and rewarding works properly for the analysed VANETs.

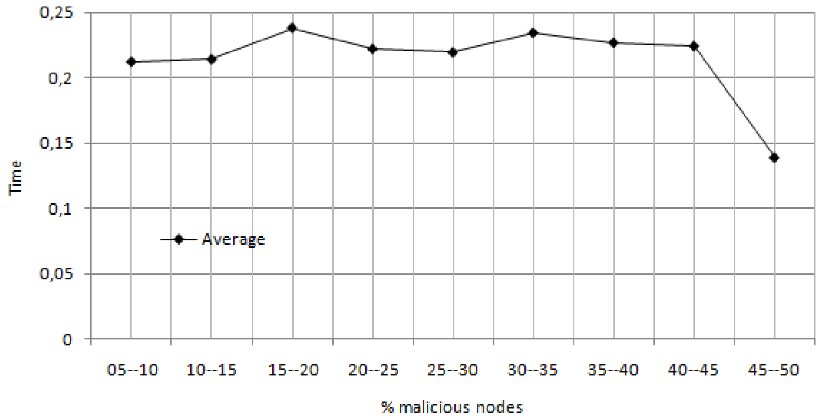

Figure 4: Average warning time vs. percentage of malicious nodes

9 Conclusions

This paper proposes several cooperation enforcement tools that provide new practical solutions for VANETs in which there is no need for any centralized authority. Thus, the aim of this work has been to develop tools to allow that a self-managed data network can be formed using existing technology so that nodes can receive and send information about traffic through their devices without the threat of lack of cooperation. This will allow addressing different security

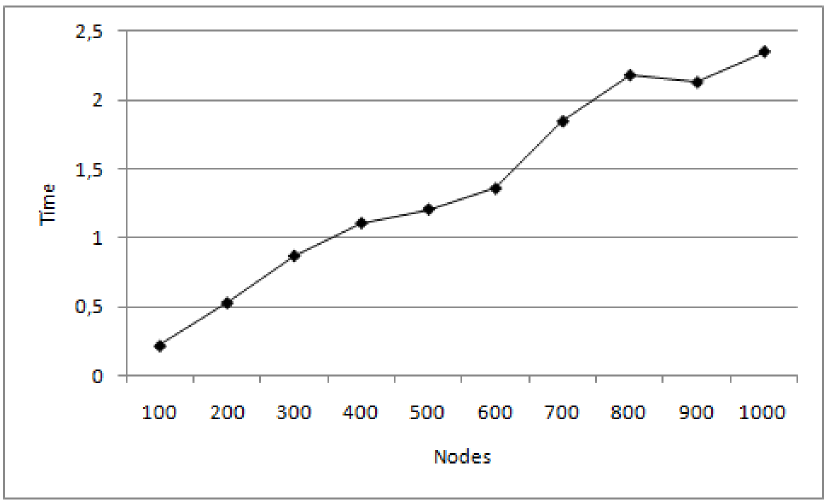

Figure 5: Average warning time vs. network size

routing and performance issues in this type of networks through free solutions based on the cooperation of users who have implemented the proposed schemes in their devices. In particular two reputation lists and acknowledgment messages as well as different mechanisms based on parameters such as time and distance have been here proposed to allow nodes to automatically detect misbehaviours in order to isolate malicious nodes. Many practical simulations of the proposal have shown its robustness and usefulness in many VANET scenarios, especially in dense conditions such as traffic congestions.

Acknowledgements

Research supported by the Ministerio Español de Educación y Ciencia and the European FEDER Fund under TIN2008-02236/TSI Project and FPI scholarship BES-2009-016774, as well as by the Agencia Canaria de Investigación, Innovación y Sociedad de la Información under PI2007/005 Project and FPI scholarship BOC Number 60.

References

[Ben Salem et al. 2006] Ben Salem, N., Buttyan, L., Hubaux, J.-P., Jakobsson, M.: "Node Cooperation in Hybrid Ad Hoc Networks"; IEEE Transactions on Mobile Computing, 5, 4 (2006), 365-376.

[Buttyan and Hubaux 2003] Buttyan, L., Hubaux, J.-P: "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks"; Journal of Mobile Networks and Applications, 8, 5 (2003), 579-592.

[Buttyan et al. 2007] Buttyan, L., Holczer, T., Vajda, I.: "On the effectiveness of changing pseudonyms to provide location privacy in VANETs"; Lecture Notes in Computer Science, 4572, Springer-Verlag (2007), 129-141.

[Buttyan and Hubaux 2007] Buttyan, L., Hubaux, J.-P: "Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing"; Cambridge University Press (2007).

[CaballeroGil et al. 2007] CaballeroGil, P., MolinaGil, C., CaballeroGil, J., Quesada-Arecibia, A.: "A simulation study of new security schemes in Mobile Ad-hoc NETworks"; Lectures Notes in Computer Science, 4739, Springer-Verlag (2007), 73-81.

[Dotzer et al. 2005] Dotzer, F., Fischer, L., Magiera, P.: "VARS: A Vehicle Ad-Hoc Network Reputation System"; Proc. Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, IEEE Computer Society (2005), 454-456.

[Fonseca and Festag 2006] Fonseca, E., Festag, A.: "A Survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETS"; Technical Report NLE-PR-2006-19, NEC Network Laboratories (2006).

[Hernández-Goya et al. 2009] Hernández-Goya, C., Caballero-Gil, P., Molina-Gil, J., Caballero-Gil, C.: "Cooperation Enforcement Schemes in Vehicular Ad-Hoc Networks"; Lecture Notes in Computer Science,5717, Springer-Verlag (2009), 429-436.

[Hubaux et al. 2001] Hubaux, J.-P., Buttyan, L., Capkun, S.: "The Quest for Security in Mobile Ad Hoc Networks"; Proc. 2nd ACM Symposium on Mobile Ad Hoc Networking and Computing (2001).

[Isaac et al. 2010] Isaac, J.T., Zeadally, S., Camara, J.S.: "Security attacks and solutions for vehicular ad hoc networks"; IET Communications, 4, 7 (2010), 894-903.

[Lee et al. 2007] Lee, S.-B., Pan, G., Park, J.-S., Gerla, M., Lu, S.: "Secure incentives for commercial ad dissemination in vehicular networks"; Proc. 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing (2007), 150-159.

[Li and Wu 2008] Li, F., Wu, J.: "A Winning-Probability-based Incentive Scheme in Vehicular Networks"; Proc. IEEE International Conference on Network Protocols (2008).

[Li and Wu 2009] Li, F., Wu, J.: "FRAME: An Innovative Incentive Scheme in Vehicular Networks"; Proc. IEEE International Conference on Communications (2009), 1-6 .

[Lo and Tsai 2009] Lo, N-W., Tsai, H-C.: "A reputation system for traffic safety event on vehicular ad Hoc Networks"; EURASIP Journal on Wireless Communications and Networking, Article ID 125348 (2009).

[Milgram 1967] Milgram, S.: "The Small World Problem"; Psychology Today, 2 (1967), 60-67.

[Mousannif et al. 2011] Mousannif, H., Khalil, I., Al Moatassime, H.: "Cooperation as a Service in VANETs"; Journal of Universal Computer Science, 17, 8 (2011), 1202-1218.

[Newman et al. 2006] Newman, M., Barabsi, A-L, Watts, D. J.: "The Structure and Dynamics of Networks"; Princeton University Press; U.S.A (2006).

[Raya et al. 2007] Raya, M., Papadimitratos, P., Aad, I., Jungels, D., Hubaux, J.-P.: "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks"; IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks, 25, 8 (2007), 1557-1568.

[Schmidt et al. 2008] Schmidt, R.K., Leinmuller, T., Schoch, E., Held, A., Schafer, G.: "Vehicle Behavior Analysis to Enhance Security in VANETs"; Proc. 4th Workshop on Vehicle to Vehicle Communications (2008).

[Sun and Fang 2008] Sun, J., Fang, Y.: "A defense technique against misbehavior in VANETs based on threshold authentication"; Proc. IEEE Military Communications Conference (2008), 1-7.

[Wang and Chigan a2007] Wang, Z., Chigan, C.: "Countermeasure Uncooperative Behaviors with Dynamic Trust-Token in VANETs"; Proc. IEEE International Conference on Communications (2007), 3959-3964.

[Wang and Chigan b2007] Wang, Z., Chigan, C.:"Cooperation Enhancement for Message Transmission in VANETs"; Journal of Wireless Personal Communications: Special Issue on Cooperation in Wireless Networks, 43, 1 (2007), 141-156.

[Xiong et al. 2010] Xiong, N., Vasilakos, A.V., Yang, L.T., Pedrycz, W., Zhang, Y., Li, Y.: "A Resilient and Scalable Flocking Scheme in Autonomous Vehicular Networks"; Journal of Mobile Networks and Applications, special issue on Advances and Applications in Vehicular Ad Hoc Networks, 15, 1 (2010), 126-136.