COOPERATIVE APPROACH TO SELF-MANAGED VANETS

J. Molina-Gil, C. Caballero-Gil and P. Caballero-Gil
Department of Statistics, Operations Research and Computing, University of La Laguna
38271 La Laguna, Tenerife, Spain

Keywords: Self-management, VANET, Cooperation, Security.

Abstract: Vehicular networks are becoming more and more important in our society because of the great benefits that can be obtained from them. Most research contributions propose specific mechanisms where the presence of a Certification Authority is necessary, which implies a centralized system in charge of certification and revocation services. In our work we propose a more realistic view of what will be the beginning of these networks, where privacy and integrity are required and where misbehaving or faulty nodes have to be detected and prevented from disrupting the network operation in a self-organized way.

1 INTRODUCTION

A Vehicular Ad-hoc NETwork (VANET) is a special type of ad-hoc network used to provide communications between On-Board Units (OBUs) in nearby vehicles, and between OBUs in vehicles and Road-Side Units (RSUs), which are fixed equipment located on the road (Yousefi, Mousavi, and Fathy, 2006). Many ideas have been proposed for vehicular networking to avoid or reduce traffic jams. However, none of them have been implemented in the real world till now.

The cryptographic needs of these networks such us authentication, data integrity, privacy and confidentiality have been analyzed in several works. To meet these needs various known mechanisms as digital signatures, hash codes or MACs and even the use of pseudonyms have been proposed. However, all these tools require Certification Authorities (CA), responsible for delivering public/private key pairs and certificates (Raya, et al. 2007). Some authors propose a Regional Transportation Authority that can be a state, province, etc. (Sun and Fang, 2008). Other authors propose a Department of Motor Vehicles (Li and Wu, 2009). However, none of these proposals are expected to be implemented in a near future.

An essential element when implementing these networks is the cooperation between vehicles because being self-managed, the exchange of messages about road conditions is vital. Therefore this paper proposes new cooperative mechanisms to ensure that the information is not lost within the network.

The rest of the paper is organized as follows. We describe the background in Section 2 and introduce our approach in Section 3. In Section 4 we provide a detailed description of the system. In Section 5 we analyse our proposal. Finally, we present our conclusions in Section 6.

2 BACKGROUND

In this network, each node is responsible for determining the authenticity of the information and reporting detected forgeries. If this happens, the forgery node will not be authenticated by anybody in the network and will be unable to get any profit from this received information. The whole process will be automatic and transparent to the network user. So, there will be a responsible module for detecting false or altered information and the information must be signed to enable nodes to determine which, is the node that presents a bad behavior, without revealing its real identity. In order to do it, pseudonyms will be used (Buttyan, Holczer and Vajda, 2007). In addition, hash functions are used as a mechanism to determine whether the information has been altered or not.

It is required that users cooperate by relaying packets to their neighboring nodes. Therefore, a possible attack could come from a passive user of the network. Such a user would benefit from getting

Molina-Gil J., Caballero-Gil C. and Caballero-Gil P. (2010).
COOPERATIVE APPROACH TO SELF-MANAGED VANETS.
In *Proceedings of the International Conference on Wireless Information Networks and Systems*, pages 94-97
DOI: 10.5220/0002991600940097

information from the network but not participate in the relay to its neighbor nodes. Consequently, we need a module to determine if nodes cooperate by relaying packets to their neighboring nodes. There exists another type of attack that consists in relaying packets to overload the network. In this case, nodes would cooperate in the attack by contributing to disseminate information that is useless or repeated. These tools to avoid such attacks and their operation will be detailed in Section 3.

During the network construction, each user must get a pair of public and private keys in a decentralized way. Additionally, a pseudonym will be given to each new node so that it will be associated to its cooperative or selfish behavior without revealing its identity. This alias will be created with an automatic generator to prevent the existence of two identical pseudonyms.

3 SYSTEM DESIGN

This design is based on a store-and-forward routing model (Li and Wu, 2008). In a typical packet forwarding process in VANETs, vehicles encounter one another at different times, and packets are opportunistically forwarded. If an intermediate vehicle stores a packet for a fixed time or actively sprays the packet to other vehicles, the packet will be more likely to reach a greater number of vehicles.

3.1 Cooperation

A bad behavior of a vehicle within a self-managed network can consist in:

- *Inserting in the network false packets* with spoofed content on the state of the road or inserting many times the same packet in search of a Denegation of Service (DoS).
- *Not cooperating in relaying packets of its neighbor nodes* so that, it benefits from the network without cooperating in its operation.

Detection of attackers should be automatic and transparent to the user. Hence, in order to detect them, the packet must contain information about management. The packets will include the following information:

- Coordinates and movement direction.
- Vehicle speed.
- TimeStamp.
- Next Via.

The coordinates combined with movement direction will provide information about the place where the packet was generated and about the traffic address where the problem is located. Besides, this will allow dropping packets generated in a certain defined range. A 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, the packet will be dropped when it reaches R. The packet will be also discarded when its TimeStamp passes. Vehicle speed will allow making decisions and altering the route to reach the destination. One parameter to detect the fastest or shortest route to the destination is the sum of all speeds in the used vias. In this sense, our system can detect whether there is a traffic jam in a specific highway and provide the speed at which vehicles move on it. This makes possible to have updated information about the road all the time. Finally, the information about the next via let us know whether the traffic jam is across the entire highway or only in a given road of the highway.

3.1.1 Detecting Misbehavior

Each vehicle must have a list where it store information on those vehicles that have reported misbehavior. This list is maintained by each node and is modified during the interaction with other vehicles. It can be updated whenever it detects a vehicle's misbehavior and when vehicles exchange packets. During the exchange of packets between two vehicles, they have to swap their lists. Thus, legitimate nodes in the network will have always an updated list so that they will not send information to nodes that have not worked on the network. Each record in this list will contain the misbehaving vehicles' pseudonyms which will allow determining who they are when they meet. The date of a bad behavior is used to keep the list updated by deleting old records. Another field with the signature of the node who presented the complaint is also stored, which allows avoiding a false allegations.

3.1.2 Characteristics

A good detection mechanism for cooperation must have the following characteristics:

- Flexibility
- Protection

With regard to flexibility, we should 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 this problem. Moreover, it would be unfair to prevent the access of

misbehaving nodes to the network forever after a bad behavior.

The protection that this facility should offer must ensure that the information that reaches the network nodes is true, which avoids 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 will compute a hash function of the packet signed with its private key and will send its public key. Thus, if the information has been altered, the intermediate node will be able to detect it. Furthermore, thanks to these detection mechanisms, selfish nodes can be isolated from the network, which ensures that those nodes involved in the network are reliable and so the information they send.

4 OPERATING MODE

Each vehicle will store a list called General Cooperation List (GCL) containing revoked pseudonyms corresponding to vehicles that have behaved badly against the operation of the network. Thus, if a vehicle has useful information about the state of the road and find another node that is within its GCL, it will not provide it with such information. Thanks to this procedure, nodes reject selfish behavior within the network. Moreover, if a node receives a packet from someone who is in its GCL, it will discard the packet so that the misbehaving node will not be able to continue attacking the network. To update these lists it is important that the process is efficient and based on a fast search algorithm. Table 1 shows four possible fields in this list.

Table 1: Possible fields of the GCL.

Selfish node's pseudonym	Selfishness date	Complainant node's pseudonym	Coordinates (X,Y)

As previously discussed, a vital aspect for the operation of the network is that nodes cooperate in relaying packets of their neighboring nodes. To meet this need, we propose the use of the Individual Cooperation List (ICL). This list will not be shared with any other vehicle in the network, as in the previous case. It allows the vehicle to store information about cooperation got from different nodes it meets during its life on the network. Also thanks to the ICL, the node can make decisions on whether to cooperate or not with other nodes. To control cooperation, an ACKnowledgment (ACK) is used, so that it is received by each node which has sent a packet. If a node A has some traffic information, before providing it to B, it will question it about B's cooperation in the network. The node B will answer with the last ACK it has received. If the date of such ACK exceeds a limit m, defined by the protocol in terms of network size, node A does not retransmit the packet. Thus the nodes will be motivated to cooperate in order to upgrade their ACKs. We could think that there might exist certain selfish behavior on the sending of the ACKs. However this is not possible due to the implementation of the protocol. Figure 1 shows in more detail this operation.

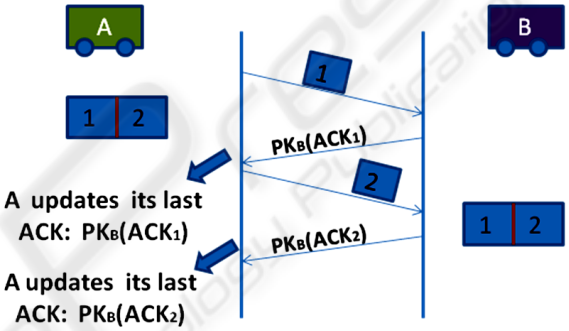

Figure 1: Sending packets and confirmation of receipt with ACK.

One node A that wants to send a packet of traffic to B, first splits it into two parts. The purpose of this split is to ensure that node A receives at least an ACK as proof that it is cooperating before B receives the complete information. So when B receives the first part of the packet, it sends the ACK signed by B (PK_B (ACK)). Then A sends to B the second part of the information so that B can recover the contents of the packet. Finally B sends the final ACK to node A.

If some of these nodes decide not to relay all necessary packets for the exchange they will be introduced in the ICL of the other detecting node.

5 ANALYSIS OF THE PROPOSAL

During the analysis of the proposed protocol, we realized that many vehicles try to profit from the network without participating in it. The cooperation mechanism described above can solve this problem. While the system cannot ensure 100% participation of the nodes in the network, it can ensure that at some point, selfish nodes try to avoid being isolated

from the network and so participate in it.

As discussed above, nodes exchange their GCLs. This implies that a node can try to attack other nodes by inserting false records in its list. Therefore we must define a criterion for determining whether a node must be isolated or not, according to its appearance in the GCLs. On the one hand a minimum number of complaints could be defined before marking a node as selfish. That is, if X nodes agree that a particular node is selfish, it is probably true. On the other hand, at least two of these complaints should have different coordinates (x,y) in order to avoid specific problems detailed below. To choose the minimum number of complaints about the same node that must be recorded before marking it like a selfish node, one possible solution would be to set this parameter as a function of the network size. Therefore, the larger the network, the greater this number must be. Another strange situation happen when a vehicle is stopped on the roadway due to an accident, car malfunction or even a phone conversation. In any of those situations, the automatic mechanism will detect a vehicle at 0 km/h on a road and send a warning about a traffic jam that does not exist. One option to solve this problem would be to revoke the car, which then should ask for a new key pair after explaining what has happened. Another solution would be to use the above idea and only revoke a node having a record of misconduct in more than one place from more than one node.

A third analyzed problem comes from the use of ACK as a cooperative mechanism. New nodes that have not participated in any retransmission will have no ACK to receive packets from the network. One solution would be that the authenticator node gives them an ACK. Another option would be to wait till the new nodes generate own packets, and after sharing them with other cars, they will get an ACK and will be able to participate in the network. The best option will be determined during the implementation of the proposal.

6 CONCLUSIONS

This paper proposes a new vision of a VANET in which there is no centralized authority. This would allow addressing all the weaknesses of this type of networks and studying whether they are viable or not. To carry out this process certain needs or security requirements must be met to obtain the contribution of the nodes that participate in it. This paper proposes cooperation tools to ensure that the information is reliable and that the nodes cooperate in relaying it. We propose two lists as well as mechanisms that allow nodes automatically to detect misbehavior. Although so far these are only ideas, the next step is the simulation and installation of a wireless network to study the speed of transmission of packets and the range of the connections.

ACKNOWLEDGEMENTS

Research supported by Ministerio Español de Educación y Ciencia and European FEDER Fund under TIN2008-02236/TSI Project, and by Agencia Canaria de Investigación, Innovación y Sociedad de la Información under PI2007/005 Project.

REFERENCES

Yousefi, S., Mousavi, M. S., Fathy, M., 2006. 'Vehicular Ad Hoc Networks (VANETs)', Challenges and Perspectives, *6th Int. conference on ITS Telecommunications*. China.

Raya, M., Papadimitratos, P., Aad, I., Jungels, D., Hubaux, J.-P., 2007. 'Eviction of Misbehaving and Faulty Nodes in Vehicular Networks'. *IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks*

Sun, J., Fang, Y., 2008. 'A defense technique against misbehavior in VANETs based on threshold authentication.', *Proc. IEEE MILCOM 2008.*

Li, F., Wu, J., 2009. 'FRAME: An Innovative Incentive Scheme in Vehicular Networks.' *Proc. of IEEE International Conference on Communications, (ICC).*

Buttyan, L., Holczer, T., Vajda, I., 2007. 'On the effectiveness of changing pseudonyms to provide location privacy in vanets ' *Proceedings of the Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS2007). Springer.*

Li, F., Wu, J., 2008. 'A Winning-Probability-based Incentive Scheme in Vehicular Networks.' *Proc. of IEEE International Conference on Network Protocols, (ICNP).*