Group Proposal to Secure Vehicular Ad-Hoc networks

J. Molina-Gil*, P. Caballero-Gil, C. Caballero-Gil

Department of Statistics, Operations Research and Computing. University of La Laguna. 38271 La Laguna. Tenerife. Spain. {jmmolina ,pcaballe, ccabgil}@ull.es

Abstract - *The main goal of VANETs (Vehicular Ad-Hoc NETwork) is to improve safety, efficiency, and comfort in everyday road travel. In a VANET, the quality of communications is degraded when the number of vehicles is very large in a small geographic area or when vehicles do not properly cooperate and forward packets for other vehicles or road infrastructure. In this paper, we address these problems and propose mechanisms that decrease the number of packets sent among vehicles and encourage collaboration in packet forwarding.*

Keywords: VANET, cooperation, groups, security.

1 Introduction

Road safety is more important every day. There are many possible situations where communications between vehicles would help to prevent accidents and to avoid collapses. A VANET is spontaneously formed by vehicles in movement and has not central infrastructure. The resulting ad hoc network offers several benefits, but requires the mobile nodes to collaborate in forwarding packets as described for ad-hoc networks in [1].

The main goal of VANETs is to improve safety, efficiency, and comfort in everyday road travel, but its structure allows taking advantage of other services such as access to Internet, commercial advices, etc. There are several general characteristics to be considered in any wireless communications network. However, when we deal with VANETs, the problems can be even greater, because of the characteristics of this kind of networks, which are composed of vehicles and infrastructures. On the one hand, this would suppose an important cost for operators to deploy all necessary infrastructures because the first solution would consist in increasing the coverage by adding antennas. Also the users should move until reaching a covered region. On the other hand, authentication, privacy, anonymity, cooperation, stability and communication delay problems appear in these changing scenarios, going from local roads without so many vehicles, to cities or highways full of vehicles.

*Contact Author.

Work submitted to SAM'10 - The 2010 International Conference on Security and Management

VANETs will support in the future a wide variety of applications, ranging from safety-related to notification and

In this paper we mainly focus on the design of schemes for the use of groups, which will considerably reduce the number of communications that take place in situations of dense traffic. Besides, we design packet forwarding enforcement schemes based on appropriate rewarding of nodes and lottery mechanisms depending on the different types of packets or traffic to be sent.

This paper is organized as follows. We introduce groups in Section 2, phases groups' details are presented in Section 3. In Section 4 we analyze groups' communication. In Section 5 and 6 we detail our cooperation enforcement scheme. Finally, we present our conclusions and future work in Section 7.

2 Group Definition

A Group in a VANET is defined as a set of vehicles that are located in a close geographic area whose formation is determined by the mobility pattern of vehicles. The group needs a minimum of vehicles and is controlled by a given node called "leader of the group". The group leader will be the one in charge of managing the information and connections. All vehicles forming part of a group have a direct wireless connection with the leader of such a group and share a secret key for their communication. Without any mechanism to minimize the number of communications, a simple broadcast will be launched from every vehicle generating a lot of unnecessary redundancy and even Denial of service (DoS). Studies [2] showing that many vehicles duplicate data packets causing collisions in the information that is sent, which degrades communication quality.

Other forms of group vehicles have been proposed for VANETs [3], [4] with different nuances and targets to our scheme. In our scheme, when the number of vehicles is low and there is no saturation of communications, the groups are not used. With a group scheme would be generated 3 connections per group for every data. The first one goes from the vehicle which produces the information to the leader, then, the leader launches a broadcast to all vehicles of the group. Finally, another connection between the leader and another vehicle (in the best position) continues broadcasting the information. Therefore it will be generated (n / number of groups) * 3 for each data packet. Vehicles will form groups according to dynamic cells where the leader is the vehicle with VANET technology that has initiated the group or that has the greatest number of neighbors when the previous leader falls below an established threshold for group formation. The

definition of these groups will be based on the average speed of the route and the direction in which vehicles circulate.

3 Group Phases

In the present work, we distinguish several phases. These phases correspond to different situations where vehicles may be, depending on the route and on their status in the moment. The proposed phases are: Detection, Election, Creation, Joining, Ending or Leader Change, and Leaving. The value of all time variables time must be chosen according to results obtained experimentally.

A. Group Detection

This is the first phase where vehicles are in normal conditions, that is to say, without dense traffic. This phase is described in Fig. 1, where neighbor(i) denotes the i-th neighbor of the node that launches the phase.

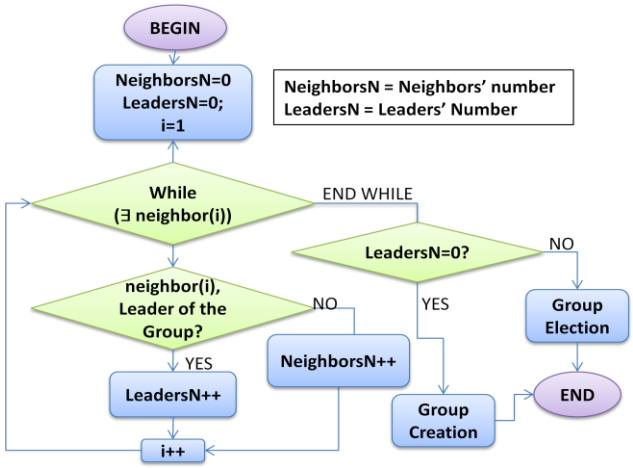

Figure 1. Group Detection

Fig. 1 shows the first phase corresponding to group formation when a vehicle checks its number of neighbors and their conditions. In case of existing at least one neighbor who is a group leader, the node proceeds either to the group election or to the group creation.

B. Group Election

In this phase the vehicle has found among its neighbors at least one node that is leader of some group. If there is only one neighbor who is a group leader, the election is automatic Otherwise, if there are several leaders, the vehicle will have to choose one of them to join it. Fig. 2 shows this phase, where groupValue denotes a quantity used for the election and groupLeader(j) represents the j-th neighbor of the node that is leader of a group.

If there are several vehicles that are leaders of some groups among neighboring nodes, the vehicle will choose one of those leaders according to the calculation of groupValue depending on:

a. The density A(j) of vehicles in each group,

b. The average quality of signal B(j) within the vehicles of each group,

c. The time C(j) that it has been connected to the leader of each group.

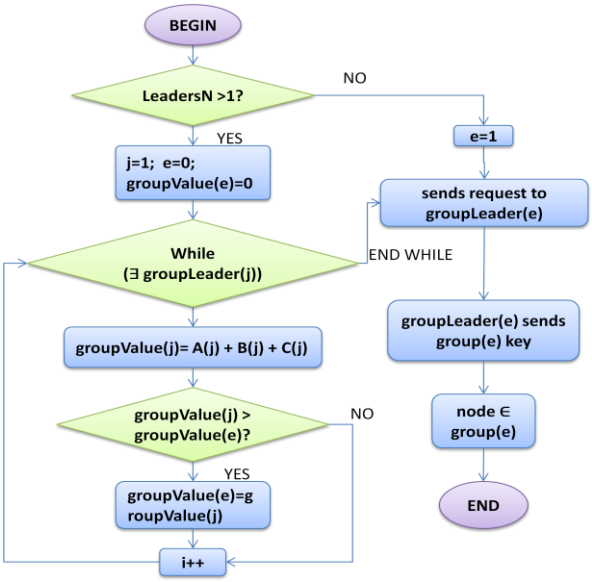

Figure 2. Group Election

These three variables A, B and C take values so that A+B+C = 1. Their ranges will be defined from tests and simulations where it will be deduced which characteristics are the most important. Once the group is chosen, the vehicle sends a joining request to the leader of the group, which after authenticating it, sends the secret key of the group encrypted with the public key of the vehicle.

C. Group Creation

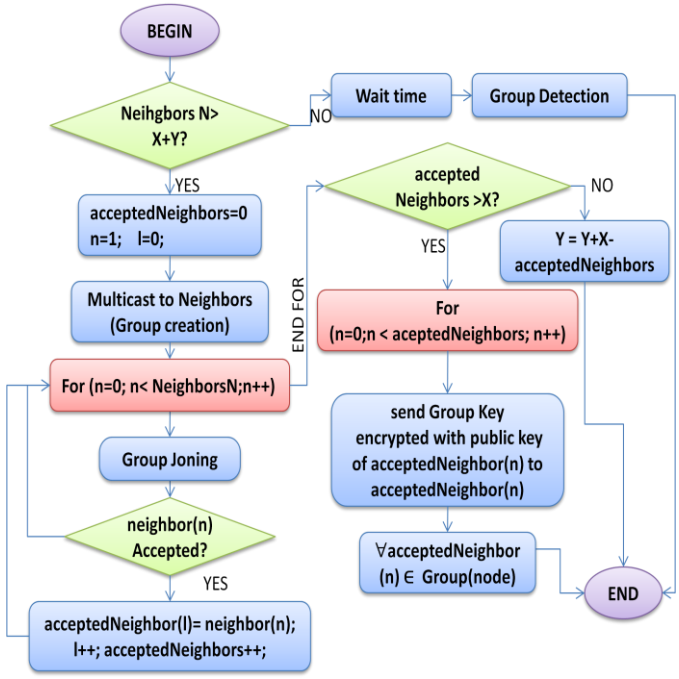

Figure 3. Group Creation

In the phase of group creation, the vehicle does not have any leader of a group nearby. Consequently, the vehicle must

check whether it has the minimum number of vehicles to form a group. Such threshold number will be a quantity X representing an estimation of the number of vehicles that will be part of the new group, plus another quantity Y that is an estimation of the number of neighbors that will not join the new group.

Fig. 3 shows that if the number of neighboring vehicles is lower than the minimum threshold required for group formation, the vehicle has to wait for a period time1 in order to begin again with group detection. Otherwise, the number of neighbors is greater than the threshold X+Y, the vehicle begins a new group creation process. To do it, it makes a multicast towards all neighboring nodes with distance equal to one by sending the group creation request. Nodes that receive this request respond accepting or rejecting the invitation after the group joining phase. If the number of neighbors that accept the invitation is greater than the minimum threshold X, the new group leader sends to each node the secret key of the group encrypted with the public keys of each node. In this moment the new group is formed.

Otherwise, the number Y of estimated vehicles is increased, by adding the number of vehicles that did not accept the invitation.

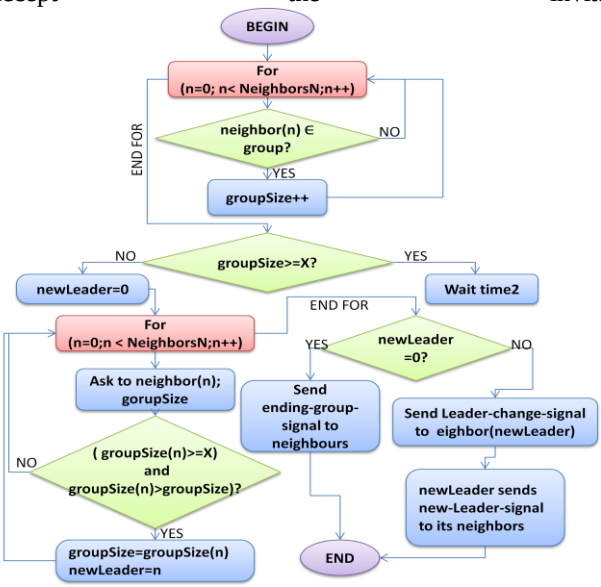

Figure 4. Group Ending or Leader Change

D. Group Joining

In the group joining phase, a vehicle receives a request for group joining. The requested vehicle basically responds yes or no depending on whether it belongs to a group or not at that moment.

If the requested vehicle does not belong to any group, it sends the acceptance answer with its public key to the vehicle that began the group creation phase. This does not mean that the group is already created. The vehicle that initiates the group creation has to check if it reaches the minimum threshold for group creation before the group is finally formed. In other case it sends non-acceptance.

E. Group Ending or Leader Change

Once the group is formed, the leader must periodically validate periodically that the group continues being useful. Otherwise, it will be necessary either to change the leader or to end the group.

Fig. 4 shows that at this phase the leader checks all neighbors belonging to its group, and if the group size is higher than X, it waits a period time2 before trying again. If the group size is less than X, then it asks every neighbor for its group size and if there are one or more neighbors that have a group size higher than X, the leader sends a Leader-Change-signal to the neighbor with the highest value. Then, this new leader sends a signal to its neighbors indicating that it is the new leader of the group. If there are no neighbors that have a group size higher than X, it represents the end of the group and consequently the leader sends an ending-group-signal to its neighbors.

F. Group Leaving

At this phase, a vehicle that belongs to a group checks whether it can see the group leader. Otherwise, the vehicle checks whether it can join another group. This phase is shown in Fig. 5.

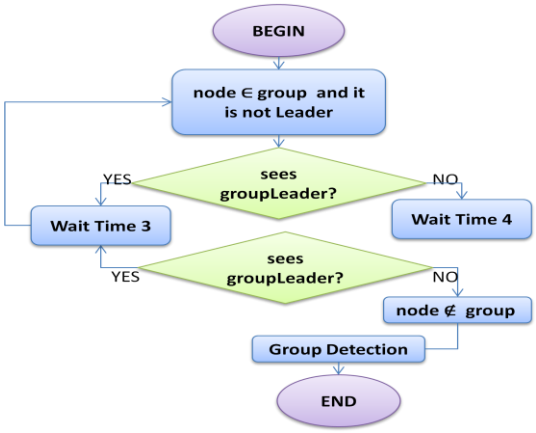

Figure 5. Group Leaving

4 Group Communications

The number of communications in VANETs when there is dense traffic is immense. For this reason, good communications management can remarkably help to improve them. In this way the number of communications will be smaller, but without missing any useful information.

In Fig. 6 the steps that a vehicle connected to a group must follow to process an input signal are explained. Before doing anything else, it must check whether the packet that it got is part of a forwarding sequence. In this case it continues the sequence and forwards the packet towards the destiny node. When the sequence is completed, the reception process ends. In case the packet is not a part of a sequence, it verifies if it is the group leader. If the data´s final destination is the vehicle, it

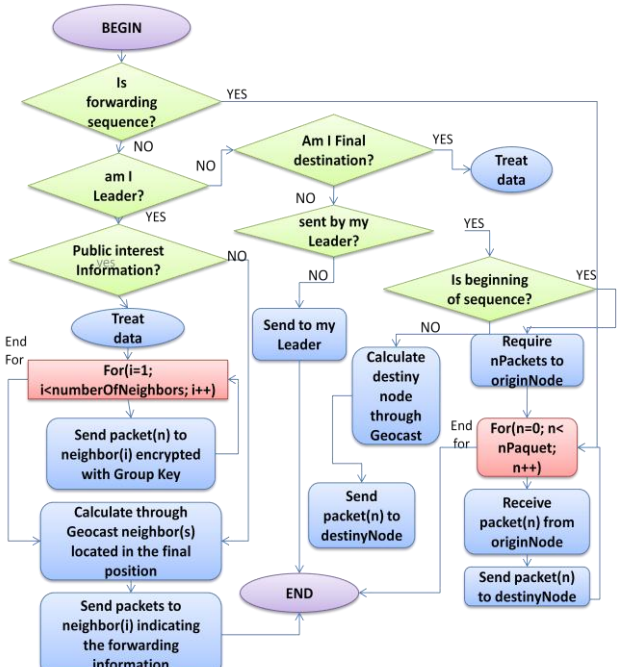

Figure 6. Communication

processes them. Otherwise, it checks if data were sent by the group leader. The group leader can send two types of packets towards any node of the group that is not the final destination of the data. They are:

1. A connection of a vehicle to Internet services, or other supplied service where it is necessary a relay of an information sequence,

2. A packet of other type of information that must be forwarded towards other parts of the network.

On the one hand, with respect to this second type of packets, there are two types of communications that must be differentiated:

- road safety information
- commercial advertising

In both of them, the vehicle that belongs to the group that receives or produces the communication, sends it to the group leader that will forward it to all connected vehicles of the group and towards the zones where the message has not been yet spread either through the vehicles of its group or other vehicles that are within the reach of the connection.

On the other hand, Internet connection can pass through another group. In this kind of connection, the intermediate nodes forward the information. If a vehicle wants to make a connection to Internet, so it makes a request towards a vehicle outside its group, which will forward the request towards its leader. The leader will send the request towards other group or the Road Side Unit, which will answer by giving details of the transmission such as the number required of packets for the connection. With this information, and knowing both the location and the speed of the vehicles of the group and the vehicle that wants to connect, the leader calculates how long is the connection between the Road Side Unit, the intermediates vehicles and the final vehicle. Then, it balances the load of connection so that the packets get to the destination vehicle as quickly as possible. Once the leader has informed the intermediate vehicles, they connect with the Road Side Unit and with the connected vehicles. After this, they relay the Internet connection.

For these types of communications, mechanisms for enforcement cooperation are necessary because without them, intermediate vehicles will not have the necessary incentives to relay others connections, what would disable any type of service that incorporates an indirect connection with the Road Side Units.

5 Cooperation Model

Our protocol uses two different schemes depending on the type of packets that are being relayed on:

- Internet Packets: This type of packets provides access to Internet.
- Advertising Packets: This type of packets provides information and advertising about shops, restaurants etc. that can be found in the geographical area coverage of the node.

In both cases it uses the idea of groups that was introduced in section II.

5.1 Internet Packets

We assume that this service has been contracted in advance with an Internet operator. Consequently, we assume that there is some user who has contracted a service, an operator that offers this service and a set of groups of vehicles that carry out the connection between the source and the destination. Nodes responsible for packets retransmission might decide not to transmit Internet packets. In this situation the operator must use some cooperation mechanism in order to provide the service to their customers. In this paper, we propose that the payment is a valuable resource for nodes, such as for example petrol. In order to obtain this valuable resource that is petrol, the nodes will be motivated to cooperate. The cost of this retransmission should be covered by the operator to which the user pays for this service. In order to perform this connection there are two different types of packets, those responsible for establishing the session between client and operator, and the individual data packets:

Establish session Packets: When an initiator A wants to communicate with Internet, it has to set up an end-to-end session with a Road-Side Unit (RSU) through one or more groups of vehicles. In order to set up a session, A generates a request message and broadcasts it. Each intermediate node in a group receiving the request, authenticate itself including a pseudonymous authentication [5], in the packet, and sends it to the leader of it group. The goal of using pseudonymous authentication is to sign messages so that the operator knows the identity of cooperative nodes and rewards them without the other relay nodes can discover it.The leader checks the

traffic information, puts its pseudonymous authentication in the packet and looks for a forwarding node in the group. When the request arrives to the RSU, it returns a session setup reply and sends a session setup confirmation message towards A. The session becomes active on the one hand for the RSU when it sends the confirmation messages and on the other hand for the vehicles when they receive a valid confirmation message .

Data Packets: Once the connection is established, data packets are retransmitted by a relaying node inside the group without having to go through the leader node. In this way, the leader will not have to receive all these data packets and can focus on its actions as leader. Before losing the connection with a base station or another group of nodes a relaying node can estimate the number of data packets that can send. Call n to this number of packets and r, significantly less than one (0< r <<1), to the reward for broadcasting each one of these packets. Therefore in a basic scheme such a node would obtain as total reward T:

$$T = r \cdot n \quad (1)$$

The operator will know who has broadcast packets because as we explained, the packets are signed by pseudonyms. It is mandatory to encrypt the contents of this package to prevent that relays nodes can read its contents.

Although the number of establishing a connection is less than the number of data packets, the reward should be the same because it is impossible to connect the source and the destination node without establishing a session. Therefore, the reward for each establishing session packets for leader nodes should be a value TL greater than r (TL > r). In section VI we will explain in detail the value of TL and how it affects the group leaders.

5.2 Ads Packets

In this case the provider sends out commercial ads, and the nearby receiving vehicles start to disseminate them to other vehicles while they are moving by using leader groups. These ads are forwarded for a certain period of time and distance from source provider. The number of generated packets is relatively higher than Internet packets because the aim of such packets is to provide advertising to as many vehicles as possible. If all vehicles were devoted to relay this type of packets without any control, the network would be overloaded, thanks to the groups idea, the leader relay them in an orderly manner. In this case, if a leader receives a packet that had previously received, it will not relay it again to its group, the result is that no nodes will receive the same packet many times from its neighbors. Hence it achieves in reducing both the number of retransmissions between groups and the number of retransmissions inside the group.

Inspired by a micro-payment scheme [6], each payment for a forwarding service can be thought as a lottery ticket. Upon receiving it, both the payee and the winner node can determine whether it is a winning ticket or not. Our model proposes a kind of lottery in which each node will have a probability Prob of being winner. The payee will not only pay to the node with the winning ticket but also to the node that received the forwarded packet. We denote by V the current node, V*i* the child nodes to that V broadcasts the ads packet. Each ad provider generates a packet which contains a unique identifier *PackID*, the ad information and a hash code *C* computed randomly with a certain size.

When a node V receives the packet, it checks the information. If V decides to participate in the forwarding, it sends the message to other nodes and waits for the receipts rec_{v_i} justifying that it has sent the packet to their children nodes V*i*. Then the node V computes for each child node rec_{v_i} a hash on PackID, NodeID and rec_{v_i} and checks the result against *C*.

$$hash\ (PackID\ |nodeID|rec_{v_i}) = C \quad (2)$$

If the equality (2) fulfills in one of these verifications, then the node V is a winner. . We denote by Probh the probability that a hash on PackID concatenated with NodeID and the receipts rec_{v_i} that child nodes send to a relaying node collides with a value

$$Prob_h(V) = Prob[\ hash\ (PackID\ |nodeID|rec_{v_i}) = C\ ] \quad (3)$$

Furthermore a node can also get a reward if it sends the winner receipt to it father. Therefore a node can transmit packets or receipts to get an award. Hence, the greater the number of retransmissions is the greater probability of winning. In this way nodes are motivated to cooperate. Moreover, this mechanism will motivate child nodes to send the receipts to node V. It is assumed that a node can receive reward for each packet it relays. So, nodes can win more than once with the same packet. The probability of a relaying node winning a prize ProbT in forwarding packets to Nc nodes, where it received the packet from a number of nodes Nf, and where we denote Vi both the Nc child nodes and the Nf father nodes of V could be defined as:

$$Prob_T(V) = \underset{N_c+N_f}{} (N_c + N_f) \cdot Prob_h - \sum_{\substack{i,j=1 \\ i \neq j}}^{N_c+N_f} Prob_h(V_i \cap V_j) + \sum_{\substack{i,j,k=1 \\ i \neq j \neq k}}^{N_c+N_f} Prob_h(V_i \cap V_j \cap V_k) - \cdots \quad (4)$$

An important aspect of using a hash function is that it may map two or more keys to the same hash value. It is called a collision. However, for the advertiser it is desirable to minimize the occurrence of such collisions. This means that the hash function must map the keys to the hash values as evenly as possible. So the advertiser should set this value and the reward to motivate nodes to participate in the broadcast, making it attractive enough.

6 The Leader Problem

It is not difficult to assume that no node wants to be leader because the number of packets they have to handle is greater than any other node belonging to the group. However, if we analyze the mechanisms used for the different types of packets we will conclude that in both cases being leader provides greater reward than being a single node in the group.

A. Internet Packets

As we discussed in section V when a session is established, the leader is in charge of finding the best route among the nodes of its group and the base station. Once this connection is established, the leader node is not longer part of this communication. However, if the leader decides not to establish the connection session, the communication would be impossible. So, the total reward received by the leader L for broadcasting and calculating the best route for Internet packets will be TL. This reward is the same than the reward of being a relay node (1) even when the amount of packets broadcast by a leader for establishing an Internet connection is much smaller than any relay node of their group. Hence the leader will be motivated to cooperate and it will want to be leader.

B. Ads Packets

As we explained in section V this model is a lottery where the ad provider must commit to provide a fixed total reward T. The vehicles that participate in the forwarding and receive a winner packet will get a share of the total reward. According to the group structure introduced in section II, a leader L will receive all ad packets in its group. Hence, it will have a bigger probability to receive a rec_{v_i} that produce a hash collision with C, so that it could be a winner node. The probability of a leader L to win a prize ProbT(L) in a group consisting of G nodes, which receive the packet from one node of the group, could be defined as:

$$Prob_T(L) = G \cdot Prob_h \quad (5)$$

In (5) it is included both what then leader can earn per receipt from their children (G-Np) and from its Np fathers. However, again the above formula implies that the leader can only win a prize per packet, which would not be correct. In that case, if the leader receives a winner receipt, it will broadcast no more packets to their neighboring nodes. To solve this problem again we should consider the probability of the union.

$$Prob_T(L) = Prob_h\ (\cup_{i=1}^{G} V_i) \quad (6)$$

Therefore, as we explained above, if the hash function minimizes the probability collisions, the expression (6) can be considered asymptotically equivalent to (5). It provides an incentive for leader to propagate ad packets, because the higher the number of retransmissions, the greater the probability of winning a reward. As leader, the packets are broadcast to all of member of its group, the model promotes that nodes prefer to be leaders, and consequently this mechanism motivates the nodes to become leaders and cooperate.

7 Conclusions

In this paper, the use of groups has been proposed as a solution to decrease the number of communications that take place in case of dense traffic since it cause a considerable drop in the quality of communication. Also we present some ideas for security cooperation mechanisms, considering two different cooperation tools. In particular, a complete description of the proposed scheme for group management in VANET is provided and the basic objective of the proposed tools for ensuring communication by using incentive and payment schemes based on lottery and reward.

This work is still to be fully developed in practice. In future versions complete simulations using the traffic simulator "SUMO" and the networks simulator "NS-2" will be described. We will analyze the operation of each phase and the connection numbers that will be avoid, comparing them with a VANET without groups. We will also calculate nodes contribution according to the VANETs' characteristics and parameters that are important both for the source node and for enforcing cooperation among nodes.

8 Acknowledgements

Research supported by Ministry of Science and Innovation and European FEDER Fund under Project TIN2008-02236/TSI and by the Agencia Canaria de Investigación, Innovación y Sociedad de la Información under PI2007/005 Project.

9 References

[1] Z. Wang, and C. Chigan, " Cooperation Enhancement for Message Transmission in VANETs" Wireless Personal Communications: An International Journal, Volume 43, Issue ,1 pp. 141-156, October 2007.

[2] O. Dousse, F. Baccelli, P. Thiran, "Impact of Interferences on Connectivity in Ad Hoc Networks," INFOCOM 2003

[3] Y. Günter, B. Wiegel, H. P. Großmann, "Medium Access Concept for VANETs Based on Clustering," VTC Fall 2007:2189-2193

[4] P. Fan, P. Sistla, P. C. Nelson, "Theoretical analysis of a directional stability-based clustering algorithm for vanets". Vehicular Ad Hoc Networks 2008:80-81

[5] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, A. Lioy "Efficient and Robust Pseudonymous Authentication in VANET" VANET 2007, Montreal, QC, Canada, September 2007

[6] M. Jakobsson, J.-P. Hubaux, and L. Buttyan. "A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks". In Proceedings of Financial Cryptography, 2003.