Cooperation in Autonomous Vehicular Networks

Sidi Mohammed Senouci[1], Abderrahim Benslimane[2], Hassnaa Moustafa[3]
[1]Orange Labs, 2 Avenue Pierre Marzin, 22307, Lannion Cedex, France
[2]LIA/CERI University of Avignon, F 339 Chemin des Meinajaries BP 1228, 84911 Avignon cedex 9, France
[3]Orange Labs, 38-40 rue General Leclerc, 92794 Issy le Moulineaux Cedex 9, France.

***Abstract*—** Vehicular networks are promising in providing Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communication, thus allowing for several useful services on roads related to safety applications as well as entertainment applications. However, a number of constraints can impact the reliability of vehicular networks applications. The general constraints concern the high mobility, dynamic environment, security of communication, and routing scalability. On the other hand, cooperation is important and beneficial for services deployment in vehicular networks. We believe that cooperation in vehicular networks could be either implicit or explicit. The former concerns the efficiency of the MAC layer protocols in order to allow reliable multi-hop transfer between the nodes, and the efficient security mechanisms (mainly authentication and access control) that could allow the different vehicles (nodes) to communicate in a trusted manner and hence cooperate in relaying each others packets. While, the latter concerns the drivers' (vehicles/nodes) behaviors, where vehicles should participate in the communication even without specific need for service access but for serving other vehicles that need relay nodes to be able to access services. In this harsh environment, innovative communication and cooperative techniques are needed. We believe that cooperative techniques can be beneficial in order to improve the performance of vehicular networks and to allow for reliable services access through those networks. In this chapter, we test this hypothesis and highlight some existing contributions in the field of cooperative autonomous vehicular networks.

***Keywords*—** Vehicular networks, Cooperation, MAC protocol, Geographical routing, Data dissemination, Clustering.

1. Introduction

Vehicular networks are considered as a novel class of wireless networks that have been emerged thanks to the advances in wireless technologies and automotive industry. Vehicular networks are spontaneously formed between moving vehicles equipped with wireless interfaces that could be of homogeneous or heterogeneous technologies. These Networks, also known as VANETs (Vehicular Ad hoc Networks), are considered as one of the ad hoc networks real-life applications enabling communications among nearby vehicles as well as between vehicles and nearby fixed equipments, usually described as roadside equipments. Vehicles can be either private, belonging to individuals or private companies, or public transportation means (e.g., buses, and public services vehicles such as police cars). Fixed equipments can belong to the government, or private network operators or service providers.

Vehicular networks applications range from road safety applications oriented to the vehicle or to the driver, to entertainment and commercial applications for passengers, making use of a plethora of cooperating technologies. This new computing paradigm is promising by allowing drivers to detect hazardous situations to avoid accidents, and to enjoy the plethora of value-added services. The increased number of vehicles on the road increases significantly the unpredictable events outside vehicles. In fact, accidents arrive rarely from vehicles themselves and mainly originate from on-road dynamics. This means that cooperation using vehicular networks must be introduced into transportation networks to improve overall safety and network efficiency, and to reduce the environmental impact of road transport.

As an example, let's take the Cooperative Collision Avoidance (CCA) application. There are two different ways to achieve cooperative collision warning: a passive approach and an active approach. In a passive approach, a vehicle broadcasts frequently its location, speed, direction, etc, and it is the responsibility of the receipt vehicle to take the decision on the eminent danger if it judges its existence. In an active approach, a vehicle causing an abnormal situation broadcasts an alarm message containing its location in order to warn vehicles in its neighborhood.

In this chapter we are exploring cooperation issues in large-scale vehicular networks, where vehicles communicate with each other and with the infrastructure via wireless links. High-level services are built following a cooperative model that depends exclusively on the participation of contributing vehicles. Hence, we will focus on the major technical challenges that are currently being resolved from cooperation perspectives for various OSI layers, such as physical and medium access control layers, network and application layers, authentication and security, etc.

The remainder of this chapter is organized as follows. Section 2 gives an overview on vehicular networks. Section 3 highlights some existing contributions in the field of cooperative vehicular networks. Finally, Section 4 summarizes and concludes the chapter.

2. Overview on Vehicular Networks

Vehicular networks can be deployed by network operators, service providers or through integration between operators, providers and a governmental authority. The recent advances in wireless technologies and the current and advancing trends in ad hoc networks scenarios allow a number of deployment architectures for vehicular networks, in highways, rural, and city environments. Such architectures should allow the communication among nearby vehicles and between vehicles and nearby fixed roadside equipments. Three alternatives include: i) a pure wireless Vehicle-to-Vehicle ad hoc network (V2V) allowing standalone vehicular communication with no infrastructure support, ii) an Infrastructure-to-Vehicle or Vehicle-to-Infrastructure (I2V, V2I) architecture with wired backbone and wireless last hops, iii) and a hybrid architecture that does not rely on a fixed infrastructure in a constant manner, but can exploit it for improved performance and service access when it is available. In this latter case, vehicles can communicate with the infrastructure either in a single hop or multi-hop fashion according to the vehicles' positions with respect to the point of attachment with the infrastructure.

Vehicular networks applications ranges from road safety applications oriented to the vehicle or to the driver, to entertainment and commercial applications for passengers, making use of a plethora of cooperating technologies. The primary vision of vehicular networks includes real-time and safety applications for drivers and passengers, allowing for these latter safety and giving essential tools to decide the best path along the way. These applications thus aim to minimize accidents and improve traffic conditions through providing drivers and passengers with useful information including collision warnings, road sign alarms and in-place traffic view. Nowadays, vehicular networks are promising in a number of useful drivers and passengers oriented services, which include Internet connections facility exploiting an available infrastructure in an "on-demand" fashion, electronic tolling system, and a variety of multimedia services.

However, to bring its potency to fruition, vehicular networks have to cope with some challenging characteristics [1] that include:

- *Potentially large scale*: As stated in the last section, most ad hoc networks studied in the literature usually assume a limited network size. However, vehicular networks can in principle extend over the entire road network and include so many participants,
- *High mobility*: The environment in which vehicular networks operate is extremely dynamic, and includes extreme configurations: in highways, relative speed of up to 300 km/h may occur, while density of nodes may be 1-2 vehicles per kilometer in low busy roads. On the other hand, in city, relative speed can reach up to 60 km/h and nodes' density can be so high, especially in rush hours,
- *Network Partitioning*: Vehicular networks will be frequently partitioned. The dynamic nature of traffic and a low penetration of the technology may result in large inter-vehicle gaps in sparsely populated scenarios, and hence in several isolated clusters of nodes,
- *Network topology and connectivity*: Vehicular networks scenarios are very different from classical ad hoc networks ones. Since vehicles are moving and changing their position constantly, scenarios are very dynamic. Therefore the network topology changes frequently as the links between nodes connect and disconnect very often. Indeed, the degree to which the network is connected is highly dependent on two factors: the range of wireless links and the fraction of participant vehicles, where only a fraction of vehicles on the road could be equipped with wireless interfaces.

- *Security*: Security is a crucial aspect in vehicular networks in order to become a reliable and accepted system bringing safety on public roads. Vehicular communication and its services will only be a success and accepted by the customers if a high level of reliability and security can be provided. This includes authenticity, message integrity and source authentication, privacy, and robustness,
- *Applications distribution*: From a general view, we can notice that building distributed applications involving passengers in different vehicles requires new distributed algorithms. As a consequence, a distributed algorithmic layer is required for managing the group of participants, and ensuring data sharing among distributed programs. Such algorithms could assimilate the neighborhood instability to a kind of fault. However, the lack of communication reliability necessitates employing fault tolerant techniques.

Several technical challenges are not yet resolved in vehicular networks. Consequently, research works and contributions are needed to investigate such challenges aiming to resolve them. We will focus on some of these technical challenges that are being resolved from cooperation perspectives. Some of our related research contributions will be also presented in the following sections.

3. Cooperation at Different OSI Layers

We are interested in designing vehicular networks protocols, for which we would like to quantify performance gains due to relaying and cooperation. In this section, we will concentrate on cooperation at the various OSI layers.

3.1 Cooperation at Lower Layers

Cooperation from MAC layer viewpoint is classified into two classes: the homogenous MAC cooperation, where one distinct MAC layer is present in the system; and the heterogeneous MAC, where MAC protocols from different systems are used for cooperation. Efficient MAC protocols [3][4] need to be in place, while adapting to the high dynamic environment of vehicular networks, and considering messages priority of some applications (ex, accidents warnings). In spite of the dynamic topology and the high mobility, fast association and low communication latency should be satisfied between communicating vehicles in order to guarantee: i) service's reliability for safety-related applications while taking into consideration the time-sensitivity during messages' transfer, and ii) the quality and continuity of services for non-safety applications.

Many MAC protocols for vehicular ad hoc networks have been introduced in the literature. But, they do not involve any cooperation between vehicles except if we consider the competition to access a given channel (as in IEEE 802.11p or DSRC) is a kind of cooperation which is not realistic. So, we have proposed a cooperative collision avoidance system which is two fold contributions, i.e., the cluster-based and risk-conscious approaches [3]. Our adopted strategy is referred to as Cluster-based Risk-Aware CCA (CRACCA) scheme. First, we have presented a cluster-based organization of the target vehicles. The cluster is based upon several criteria, which define the movement of the vehicles, namely the directional bearing and relative velocity of each vehicle, and also the inter-vehicular distance. Second, we have designed a cooperative risk-aware Media Access Control (MAC) protocol in order to increase the responsiveness of the proposed CCA scheme. According to the order of each vehicle in its corresponding cluster, an emergency level is associated with the vehicle that signifies the risk to encounter a potential emergency scenario. In order to swiftly circulate the emergency notifications to collocated vehicles for mitigating the risk of chain collisions, the medium access delay of each vehicle is set as a function of its emergency level.

3.2 Cooperation at Network Layer

Cooperation from a network viewpoint concerns the cooperation mechanisms between network elements for traffic forwarding. More specifically, it is about the design of an efficient routing protocol that enables effective network resource management [5][6]. We note that it is important to study the node behavior in the case of infrastructure-less vehicular networks. In fact, in such networks, where no centralized entity exists, a malicious or self-interested user can misbehave and does not cooperate. A malicious user could inject false routing messages into the network in order to break the cooperative paradigm. The basic vehicular network functions subject to selfishness are dissemination and routing. For our propositions dealing with cooperative routing protocols and presented afterward, we considered that all vehicles are not selfish and cooperate to route data for the others.

Furthermore, vehicular networks face a number of new challenges like scalability and high mobility. An effective solution is also to define a robust self-healing and self-organizing architecture that facilitates the cooperation between vehicles. Depending on the application, this cooperation will be based on either proactive or reactive self-organization architecture [7][8] . The two architectures are cross layer and structure intelligently the vehicular network in permanent manner by portioning roads into adjacent segments seen as geographic fix clusters.

In the following, we give details of some of these network protocols and quantify performance gains due to relaying and cooperation.

3.2.1 Cooperative Routing in Vehicular Networks

In vehicular networks consisting of distributed vehicles, the information is routed from the source node to the destination node using intermediate nodes in a multi-hop fashion. These intermediate nodes cooperate with each other in transmitting the information, and through this cooperation effectively enhance the end-to-end delay. It is important to use the best intermediate nodes when multiple nodes exist in the transmission [14][15]. Several questions arise in this context: What level of coordination among the cooperating nodes is needed? And how must the route selection be done to minimize the end-to-end delay? These are the problems that we look at here. We develop a formulation that captures the benefit of cooperative transmission and develop a routing algorithm for selecting the optimal route under this setting.

Topology-based and position-based routing are two strategies of data forwarding commonly adopted for vehicular networks. The increasing availability of GPS equipped vehicles makes position-based routing a convenient routing strategy for these networks. Several variants of position-based concept have been proposed for data forwarding in vehicular networks [16]-[22]. Three classes of forwarding strategies can be identified for position-based routing protocols: 1) restricted directional flooding, 2) hierarchical forwarding, and 3) greedy forwarding [5]. Most of these protocols do not take into account the vehicular traffic, which means that such algorithms may fail in case they try to forward a packet along streets where no vehicles are moving. Such streets should be considered as 'broken links' in the topology. Moreover, a packet can be received by a node that has no neighbors nearer to the receiver than the node itself. In this case, the problem of a packet having reached a local maximum arises. These problems can be overcome to some extent knowing the real topology, by opting to use only streets where vehicular traffic exists. In addition, in [21], forwarding a packet between two successive intersections is done on the basis of a simple greedy forwarding mechanism. This classic greedy approach works well since it is independent of topological changes but it suffers from inaccurate neighbor tables since it does not consider the vehicle direction and velocity. Thus, it may be possible to lose some good candidate nodes to forward the packets. Our objective was to conceive a routing protocol that overcomes the above limitations.

We proposed GyTAR (improved Greedy Traffic Aware Routing protocol) [5][6]; an intersection-based geographical routing protocol, capable to find robust and optimal routes within urban environments. GyTAR scheme is organized into three mechanisms: (i) a mechanism for the dynamic selection of the intersections through which packets are forwarded to reach their destination, and (ii) an improved greedy forwarding mechanism between two intersections. Using GyTAR, packets will move successively closer towards the destination along the streets where there are enough vehicles providing connectivity. We do not impose any restriction to the communication model, and GyTAR is applicable to both completely ad hoc and infrastructure-based routing.

For the first mechanism "Intersection selection", GyTAR adopts an anchor-based routing approach with street awareness. Thus, data packets are routed between vehicles, following the street map topology. However, unlike GSR [20] and A-STAR [21], where the sending node statically computes a sequence of intersections the packet has to traverse in order to reach the destination, intermediate intersections in GyTAR are chosen dynamically and in sequence, considering both the variation in the vehicular traffic and distance to destination. Partial successive computation of the path has a threefold advantage: (i) the size of packet header is fixed; (ii) the computation of subsequent anchors is done exploiting more updated information about vehicular traffic distribution; (iii) subsequent anchors can be computed exploiting updated information about the current position of the destination. When selecting the next destination intersection, a node (the sending vehicle or an intermediate vehicle in an intersection) looks for the position of the neighboring intersections using the map. A score is attributed to each intersection considering the traffic density and the curvemetric distance[1] to the destination. The best destination intersection (i.e., the intersection with the highest score) is

[1] This term describes the distance measured when following the geometric shape of a road.

the geographically closest intersection to the destination vehicle having the highest vehicular traffic. After determining the destination intersection, the second mechanism "improved greedy strategy" is used to forward packets towards the intersection. For that, all data packets are marked by the location of the next intersection. Each vehicle maintains a neighbor table in which the velocity vector information of each neighbor vehicle is recorded. Thus, when a data packet is received, the forwarding vehicle predicts the position of each neighbor using the corresponding recorded information (velocity, direction, and the latest known position), and then selects the next hop neighbor (the closest to the destination intersection). Note that most of the existing greedy-based routing protocols do not use the prediction and consequently, they might lose some good candidates to forward data packets. Despite the improved greedy routing strategy, the risk remains that a packet gets stuck in a local optimum (the forwarding vehicle might be the closest to the next intersection). Hence, a recovery strategy is required. The recovery strategy adopted by GyTAR is based on the idea of '*carry- and-forward*' [23]: the forwarding vehicle of the packet in a recovery mode will carry the packet until the next intersection or until another vehicle, closer to the destination intersection, enters/reaches its transmission range.

GyTAR efficiently utilizes the unique characteristics of cooperative vehicular environments like the highly dynamic vehicular traffic, road traffic density as well as the road topology in making routing and forwarding decisions. The selection of intermediate intersections among road segments is performed dynamically and in-sequence based on the scores attributed to each intersection. The scores are determined based on the dynamic traffic density information and the curvemetric distance to the destination. Simulation results showed that GyTAR performs better in terms of throughput, delay and routing overhead compared to other protocols (LAR and GSR) proposed for vehicular networks. The robust intersection selection and the improved greedy carry-and-forward scheme with recovery, suggests that GyTAR should be able to provide stable communication while maintaining high throughput and low delays for vehicular routing in urban environments.

Cooperation between vehicles can also help a given vehicle to access Internet. When a node in a vehicular ad hoc network wants Internet access, it needs to obtain information about the available gateways and it should select the most appropriate of them. Exchanging information messages between vehicles and gateways is important for V2I. We can distinguish three different approaches to discover gateways: (i) Proactive gateway discovery, (ii) Reactive gateway discovery, and (iii) Hybrid gateway discovery. To connect vehicles to Internet, our objectives are to reduce the overhead during the gateway discovery process, create a relatively robust network, and make the handovers seamless. We suggested a hybrid gateway discovery process that restricts broadcasts to a pre-defined geographical zone, while letting only some relays re-broadcast the advertised messages [40]. Stability metrics (e.g., speed, direction and location) of vehicles can help us to predict the future location of vehicles, and the period that they stay in the transmission range of each other. We applied this information to estimate the link lifetime, and recursively the lifetime of routes from vehicles to gateways. Vehicles select the most stable route to gateways, and extend the lifetime of their connection. The most stable route is not necessarily the shortest one, it is the path with the longest life time. Here we are more interested in the life time of the connection rather than the number of hops to the destination. Having a list of routes to different gateways, a vehicle can hand-over the connection to the next available gateway before the current connection fails. If a vehicle does not receive advertisement messages, it should start sending out solicitation messages to find a new gateway. Internet access is provided by gateways implemented in roadside infrastructure units, and vehicles initially need to find these gateways to communicate with them. Gateway discovery is the process through which vehicles get updated about the neighboring gateways. Gateways periodically broadcast gateway advertisement messages in a geographically restricted area using geocast capabilities. Gateway discovery aims at propagating the advertisement messages in VANET through multiple hops in this area. We call this area the broadcast zone of a gateway: a message that originated from that gateway should not be broadcasted outside this zone. This area can be a rectangle or a circle1, and is defined according to the distance between gateways, transmission range of the gateways, and density of the vehicles (whether it is a highway or city, traffic congestion, etc). For instance, suppose that the broadcast zone is selected to be a circle. Gateways send their location (xg, yg), as the center of this circle, and a predefined radius along with the advertisement messages. Upon receiving the message, vehicles extract this information and can perceive if they are located inside our outside of the broadcast zone of a gateway.

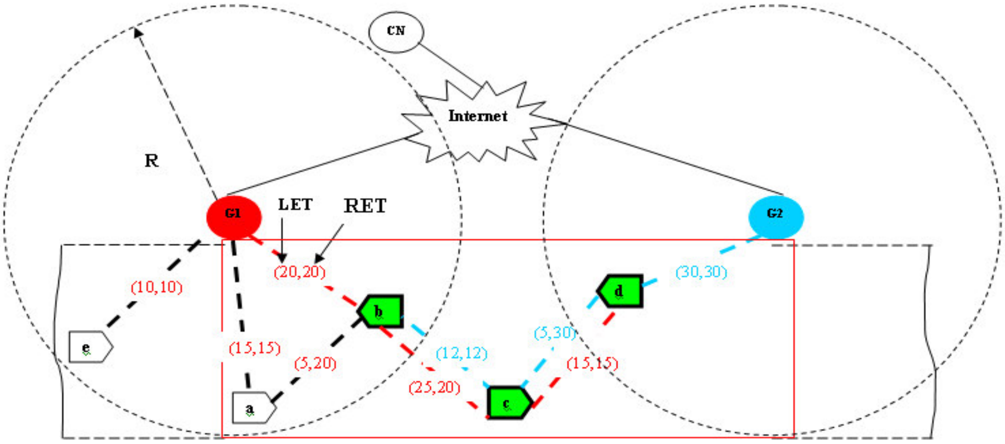


Figure 1. A Gateway broadcasting an advertisement message. Transmission range R and broadcast zone of gateway G1 is shown. On the links, a couple of values (LET, RET) means (link expiration time, route expiration time). CN means the correspondent node (as in Mobile IP).

To accomplish the task of proactive gateway discovery, we consider Optimized Dissemination of Alarm Messages (ODAM) [9], which is based on geographical multicast, and consists of determining the multicast group according to the driving direction and the positioning of the vehicles in a geographically restricted area using geocasting capabilities. These messages are then re-broadcasted in the network by some particular nodes called relays. Figure 1 shows a simple scenario, in which gateway 1 starts to broadcast advertisement messages to neighboring vehicles. The broadcast zone is considered as a rectangle here, and has an intersection with the transmission range zone of gateway 2. In this case, messages from gateway 1 will be broadcasted through multi hops to some of the nodes which are connected to gateway 2. Each advertised message contains the gateway address, relay address, message sequence number, broadcast zone, and the stability parameters. Stability parameters (sender position, sender speed, sender direction, and the estimated route expiration time) are used by each vehicle receiving the message to predict the link lifetime.

3.2.2 Cooperative Dissemination in Vehicular Networks within City Environment

Many of vehicular network applications rely on disseminating data, e. g., on the current traffic situation, weather information, road works, hazard warning, etc. Typically, such applications are based on some form of proactive information dissemination in an ad hoc manner. Proactive information dissemination is, however, a difficult task due to the highly dynamic nature of vehicular networks. Indeed, vehicular networks are characterized by their frequent fragmentation into disconnected clusters that merge and disintegrate dynamically. One of the largely accepted solutions towards efficient data dissemination in vehicular networks is by exploiting a combination of fixed roadside infrastructures and mobile in-vehicle technologies. There are some recent examples of broadcasting protocols specifically designed for vehicular networks with infrastructure support [24][25]. While such infrastructure-based approaches may work well, they may prove costly as they require the installation of new infrastructures on road network, especially if the area to be covered is large.

In this context, our contribution was to propose a self-organizing mechanism to emulate a geo-localized virtual infrastructure (GVI) by a bounded-size subset of cooperating vehicles populating the concerned geographic region [26]. This is realized in an attempt to both approaching the performance of a real infrastructure while avoiding the cost of installing it. As we are dealing with the city environment, an intersection sounds suitable as geographic region because of its better line-of-sight and also because it is a high traffic density area. Hence, the proposed GVI mechanism can periodically disseminate the data within a signalized (traffic lights) intersection area, controlled in fixed-time and operated in a range of conditions extending from under-saturated to highly saturated. Thus, it can be used to keep information alive around specific geographical areas [27] (nearby accident warnings, traffic congestion, road works, advertisements and announcements, etc.). It can also be used as a solution for the infrastructure dependence problem of some existing dissemination protocols like ODAM [9].

The geo-localized virtual infrastructure mechanism consists on electing vehicles that will perpetuate information broadcasting within an intersection area. To do so, the GVI is composed of two phases: (i) selecting the vehicles that are able to reach the broadcast area (i.e. a small area around the intersection center, where an elected vehicle could perform a local broadcast); then, (ii) among the selected vehicles, electing the local broadcaster which will perform a local single-hop broadcast once it reaches the broadcast area (i.e. at the intersection center).

In the first phase and as shown in the next figure, among the vehicles which are around the intersection, only those within the notification region A_i (a cell centered on C_i and delimited by a ray of $R/2$ where R is radio range) could participate to the local broadcast. They are selected as candidates if they are able to reach the intersection center C_i. In the second phase, a waiting time is assigned to each candidate vehicle. This waiting time considers the geographical location, direction and speed of the vehicle and also the desirable broadcast cycle time T of GVI. The candidate vehicle with the shortest waiting time will broadcast a short informative message telling other candidate vehicles that it has been elected as the local broadcaster.

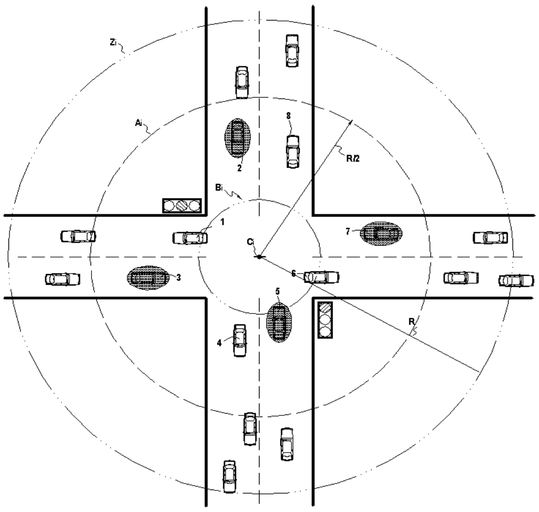


Figure 2. Selecting vehicles candidates in the GVI mechanism.

Analytical and simulation results show that the proposed GVI mechanism can periodically disseminate data within an intersection area, efficiently utilize the limited bandwidth and ensure high delivery ratio. More precisely, with varying the broadcast cycle time T, we can have a kind of compromise between two metrics, namely the number of copies of the same message (which corresponds to a measure of the cost to provide the service) and the probability to inform a vehicle (which corresponds to a measure of quality of service). Indeed, if we want that all vehicles receive the message, we should decrease the broadcast cycle time value which will generate an overhead. However, we can minimize the number of copies of the same broadcast message received by a vehicle as long as we tolerate the fact that certain vehicles fail to receive the message. Analytical models showed that that GVI fails only when the traffic density is extremely low and no sufficient cooperative vehicles within the intersection.

3.2.3 Cooperative Dissemination in Vehicular Networks within a Highway

Cooperative Collision Warning (CCW) is an important class of safety applications that target the prevention of vehicular collisions using vehicle-to-vehicle (V2V) communications. In CCW, vehicles periodically broadcast short messages for the purposes of driver situational awareness and warning. However, a classical broadcast cannot be used since it causes a protocol overhead and high number of message collisions which can be harmful for the safety of drivers. To overcome this limitation, we introduced an Optimized Dissemination of Alarm Messages (ODAM) [9] while restricting re-broadcast to only special nodes, called relays, and in restricted regions, called risk zones.

ODAM works as follow. When a crash occurs, a damaged vehicle or any other vehicle which detects this problem must broadcast an alarm message to inform the other vehicles about the danger. Several methods were used for the crash detection. For example, when an accident occurs, the activation of the airbag can initiate the alarm message broadcast. Among all the neighbors of this vehicle, only those which are in the risk zones take into account the message (Figure 3). Vehicles in these risk zones constitute a dynamic multicast group. Among all neighbors in the same zone, only one vehicle, called relay, must react to ensure the rebroadcast of the alarm message to inform vehicles which did not receive the message yet. The relay is completely selected in a distributed way. Each vehicle can know, from the transported information in the alarm message which it receives, if it will become relay or no. Moreover, the relay must be selected in order to ensure the coverage of the greatest zone not yet covered by the sender. Consequently, the relay must be the furthest neighbor away from the sender.

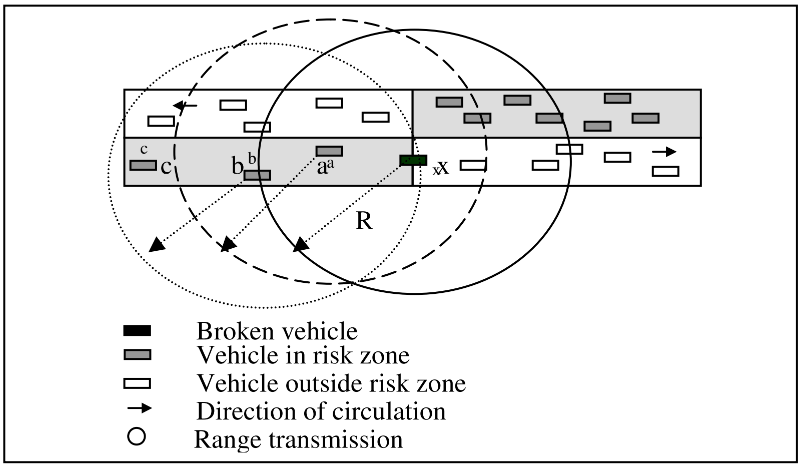


Figure 3. Relevant areas and relay selection in ODAM.

In figure 3, a damaged vehicle (x) broadcasts an alarm message. We remark that if the vehicle (a) were taken as relay, then (c) cannot be reached because it was out of the transmission range of (a). Against, if (b) were selected as relay, then (c) would have been reached and informed. A relay is designated as the vehicle having the minimum value of computed defertime. The vehicle which receives an alarm message should not rebroadcast it immediately but must wait during a defertime. The defertime value is inversely proportional to the distance from the sender to the receiver. At the expiration of this time, if a node does not receive another alarm of the same message, coming from another node, then it rebroadcast the message. By this, it is chosen as relay.

To favour the furthest vehicle from the sender to becoming relay, defertime of each vehicle must be inversely proportional to the distance which separates it from the sender. As the distance between these two vehicles is large as defertime is small. The value of defertime(x), computed by a vehicle (x) receiving a message and which is candidate to retransmit it, is given by the following formula:

$$defertime(x) = \max\_defer\_time \cdot \frac{(R^{\varepsilon} - D_{sx}^{\varepsilon})}{R^{\varepsilon}} \qquad (1)$$

where ε is a positive integer.

If we suppose that the distribution of the vehicles is uniform, the choice for $\varepsilon = 2$ will give a uniform distribution of the various values of defertime in [0, max_defer_time]. D_{sx} is the distance between the sender (s) and the receiver (x). The value of max_defer_time is equal to twice the average of communication delay.

For each received message, the vehicle must determinate its location in report with the broken vehicle. Indeed, we presented in [9] a technique to compute a vehicle location with GPS. Also, it allows to determinate the direction of circulation and position in report with the broken vehicle. Thus, this technique allows to restrict the broadcast to the only relevance zones.

A study of broadcast enhancement techniques for CCW applications over Dedicated Short Range Communication (DSRC) reveals interesting trade-offs inherent to the latency perceived by periodic broadcast safety applications [10]. A broadcast based packet forwarding mechanism is proposed in [11] for intra-platoon cooperative collision avoidance using DSRC MAC protocol. An implicit acknowledgement mechanism was introduced for reducing the amount of broadcast traffic for enhanced packet delivery rate. Due to a high frequency of link breaks, a standard approach cannot cope with high mobility. A recent approach based on virtual routers has been proposed to address this problem. In this new environment, virtual routers are used for forwarding data. The functionality of each virtual router is provided by the mobile devices currently within its spatial proximity. Since these routers do not move, the communication links are much more robust compared to those of the conventional techniques. To enforce collaboration among mobile devices in supporting the virtual router functionality, some techniques are investigated in [12]. These techniques are Connectionless approaches for Street (CLA-S). According to application requirements, authors in [13] design a vehicle-to-vehicle communication protocol for cooperative collision warning. It comprises congestion control policies, service differentiation mechanisms and methods for emergency warning dissemination.

3.2.4 Self-Organizing Cooperative Vehicular Networks

To overcome some of the challenges that face a vehicular network, a self-organizing architecture has to be set up to simplify the network management task and to permit the deployment of a lot of services. The term "Self-organization" has been introduced in the 60's in cybernetics and in the 70's in physics of complex systems. It is described as a mechanism through which individual elements in a group cooperate locally yet give the group a macroscopic property, often described as an organization or a structure. This architecture should take advantage of vehicle properties to issue a global virtual structure enabling the network self-organization. It should be sufficiently autonomous and dynamic to deal with any local change.

Most researches suggest virtual backbone [28] and clustering [29] as most efficient structures to self-organize the mobile ad hoc networks and to achieve scalability and effectiveness in broadcasting. The idea of defining a virtual backbone structure is brought from the wired networks. The principle of this solution is to constitute a dorsal of best interconnected nodes. The other nodes will be associated with the dorsal nodes. The constraint is the judicious choice of backbone members to avoid the rapid loss of interconnection between them. The second self-organizing structure is clustering where "*vehicles-cooperation*" is used to group the nodes into homogeneous groups named clusters. Each cluster has at least one cluster head and many members. Cluster-based solutions represent a viable approach in propagating messages among vehicles. Thus, the clustering structure is usually used as a support of backbone structure.

We proposed CSP (Cluster-based Self-organizing Protocol) [7][8]; a vehicular network proactive self-organizing architecture that is based on geographical clustering to ensure a permanent self-organization of the whole network. The key idea is to divide each road stump in segments seen as fixed clusters and electing a cluster head for each segment to act as backbone member. CSP adapts itself to vehicular network characteristics and permits to improve inter-vehicles or vehicle-to-infrastructure connectivity without producing a great overhead.

We demonstrated that CSP facilitates the network management task and permits to deploy wide panoply of services. For example, it allows telecommunication/service providers to better exploit/extend the existing infrastructure by overcoming its limitations using cooperative vehicles. We demonstrate via simulations that CSP is optimal when using an advertisement diffusion application on the top of it. In addition CSP does not generate a great routing overhead since it relies on fix segments to organize the network.

3.3 Security and Authentication versus Cooperation

Cooperation between nodes in vehicular networks should be guaranteed in order to assure the correct service provision. Although cooperation in vehicular networks is important and beneficial to allow service access in a multi-hop distributed fashion, it could penalize the service access and the whole communication if malicious nodes could be involved in the communication. To assure secure and hence reliable cooperation, it should be ensured that only authorized users are granted network's access.

Two main types of attacks could exist in vehicular networks and could allow non-cooperative behavior in such environment: i) external attacks, where the attackers do not participate in the network, however they could carry out some attacks and malicious acts impacting the communication and the network and services performance, and ii) internal attacks, where the attackers participate in the network and have legitimate service access, however they penalize the network performance through malicious and non cooperative acts. Consequently, efficient counter measures against these attacks need to be employed in order to ensure secure and reliable cooperation in vehicular networks. These counter-measures includes authentication and access control that are important counter-attack measures in vehicular networks deployments, allowing only authorized users to have connectivity. Although authentication and access control can reinforce cooperation through prevention against external attackers, internal attackers could always exist even in the presence of effective authentication and access control mechanisms. Internal attackers are nodes that are authenticated and authorized to participate in the network; however, they can be harmful nodes causing network and service performance degradation mainly through non cooperative behaviors (selfishness, greediness, and Denial-of-Services or DoS). Hence, there is a need for complementary mechanisms to authentication and access control.

Prevention Against External Attacks. Indeed, authentication and access control are important counterattack measures in vehicular networks deployments, allowing only authorized clients to be connected and preventing external attackers to sneak into the network disrupting the normal cooperative operation or service provisioning. A simple solution to carry out authentication in vehicular networks is to employ an authentication key shared by all nodes in the network. Although this mechanism is considered as a *plug and play* solution and does not require the communication with centralized network entities, it is limited to closed scenarios of small number of participants in limited environments and belonging to the same provider. In addition, this shared secret authentication has two main pitfalls. Firstly, an attacker only needs to compromise one node to break the security of the system. Secondly, mobile nodes do not usually belong to the same community, which leads to a difficulty in installing/pre-configuring the shared keys. A challenge for wide scale services deployment in vehicular networks is to design authentication mechanisms for the more vulnerable yet more resource-constrained environment of vehicular networks having multi-hop ad hoc communication. In most commercial deployments of WLANs, authentication and access control is mostly provided through employing IEEE 802.11i (IEEE 802.11i, 2004) authentication in which a centralized server is in place. In the context of vehicular networks, the challenge for applying the 802.11i approach mainly concerns the multihop characteristics and the hybrid infrastructurebased/less architecture. Hence, the 802.11i authentication model should be adapted to such environment through mainly considering two issues: i) introducing distributed authentication mechanisms, and ii) ensuring cooperation between nodes to support the hybrid architecture.

A possible approach for distributed authentication is the continuous discovery and mutual authentication between neighbors, whether they are mobile clients or fixed APs/BSs. Nevertheless, if mobile nodes move back to the range of previous authenticated neighbors or fixed nodes, it is necessary to perform re-authentication in order to prevent an adversary from taking advantage of the gap between the last security association and the current security association with the old neighbor. An approach adapting the 802.11i authentication model to multihop communication environments is presented in [30], proposing an extended forwarding capability to 802.11i and allowing mobile node authentication with the authentication server in a multihop fashion. The notion of friend nodes is introduced allowing each mobile node to initiate the authentication process through a selected node in its proximity, which plays the role of an auxiliary authenticator and forwards securely the authentication requests to the authentication server. Friend nodes are chosen to be trusted and cooperating nodes. This approach is suitable to the hybrid infrastructure-based/less architecture in vehicular networks, allowing mobile nodes beyond the APs/BSs coverage zone to get authenticated in a cooperative manner, through communicating with the authentication server at the infrastructure while passing by cooperative nodes (friend nodes). In addition, this approach allows authentication keys storage among intermediate (friend) nodes which optimizes the re-authentication process in case of roaming.

In addition, [31] presents a distributed authentication and services' access control solution for services' commercialization in ad hoc networks with a possible application to vehicular networks environments. This work extends the Kerberos authentication model to provide each mobile node with a number of keys that are encapsulated in the Kerberos authentication ticket and are based on the sliding interval principle, where each key is only valid for a certain interval of time. Consequently, each pair of communicating nodes could authenticate and setup a secure link if they share the key that corresponds to the interval of communication and hence could cooperate for relaying each others packets during services access. The number of keys obtained by each node reflects the nodes duration for services' access. In addition, the Kerberos services' tickets are used by each node to authorize access to the corresponding services.

Another possibility to facilitate multihop authentication is to employ a Protocol for carrying Authentication and Network Access or PANA [32]. PANA allows the encapsulation of the used authentication protocol messages and their routing to the authentication server. The advantage of PANA mainly lies in its independence of the wireless media, and thus it is suitable for future vehicular networks allowing cooperation between heterogeneous deployments and operator co-existence. However, PANA necessitates the existence of a routing infrastructure, which is a technical challenge in cooperative vehicular networks as previously outlined.

Prevention Against Internal Attacks. Although authentication and access control can reinforce cooperation through prevention against external attackers, internal attackers could always exist even in the presence of effective authentication and access control mechanisms. Internal attackers are nodes that are authenticated and authorized to participate in the network; however, they can be harmful nodes causing network and service performance degradation mainly through non cooperative behaviors (selfishness, greediness, and Denial-of-Services or DoS). Hence, there is a need for complementary mechanisms to authentication and access control. Nodes may behave selfishly by not forwarding packets for others in order to save power, bandwidth or just because of security and privacy concerns. Watchdog [33], CONFIDANT [34] and Catch [35] are three approaches developed to detect selfishness and enforce distributed cooperation and are suitable for vehicular networks multihop environment. Watchdog is based on monitoring neighbors to identify a misbehaving node that does not cooperate during data transmission. However, CONFIDANT and Catch incorporate an additional punishment mechanism making misbehavior unattractive through isolating misbehaving nodes. On the other hand, nodes may behave greedily in consuming channel and bandwidth for its own benefits at the expense of the other users. The DOMINO mechanism [36] solves the greedy sender problem in 802.11 WLANs with a possible extension to multihop wireless networks and hence vehicular networks. Internal attackers may also cause DoS through either faked messages injection or messages replay. DoS is a challenging problem greatly impacting cooperation, however it could be partially resolved through effective authentication of messages and messages' sources.

3.4 Cooperation at Upper Layers

Several cooperative applications are based on cooperation between vehicles and the infrastructure belonging to the government, or private network operators or service providers. Based on the CVIS project [37], these services fall under three main categories: *urban*, *inter-urban* and *freight and fleet management*.

1. *CURB - Cooperative Urban Applications*: aims to improve the efficient use of the urban road network at both local junction and network level, and enhance individual mobility. Main innovation will be the cooperative exchange of data between individual vehicles and the roadside equipment, and provision of dedicated, targeted services to individual vehicles from the roadside. This will create a cooperative system for detailed travel data collection, personalized travel information, greatly improved management of traffic at all urban levels and promote the efficient use of road space. Four applications are developed in CVIS: (i) Cooperative Network Management: Optimum area traffic management by using vehicle/driver destination and other characteristics, and individualized route guidance, (ii) Cooperative Area Routing: Intersection controllers signal momentary disturbances in traffic flow in their area of control, and give individual, destination-based and appropriate rerouting advice to approaching vehicles, (iii) Cooperative Local Traffic Control: Enhanced local intersection traffic control that cooperates with the approaching vehicles, gives control and traffic state related information to the driver and supports and creates green waves through speed recommendations (profiles) for the drivers and data exchange with neighboring intersections, and (iv) Cooperative Flexible Lane Allocation: To increase the capacity of the road infrastructure, a dedicated bus lane is made available to "licensed" and CVIS-equipped vehicles, travelling in the same direction, allowing them to use the lane when and where it would not be a nuisance to public transport and the arguments of speed, punctuality and economy would not be compromised.

2. *CINT - Cooperative Inter-urban Applications*: aims to enable cooperation and communication between the vehicle and the infrastructure on inter-urban highways. It will develop and validate cooperative services to improve the efficiency, safety and environmental friendliness of traffic on the inter-urban road network and offer a safe and comfortable journey to drivers and passengers. Two applications are developed in CVIS: (i) Enhanced Driver Awareness (EDA): This application focuses on safety and will Inform vehicle drivers within 5 seconds by communication from the roadside or even nearby motorists, about relevant aspects of the dynamic traffic situation, current speed and other regulations, road and weather conditions downstream, also offering the possibility to enhance the effectiveness of in car systems for driver assistance, and (ii) Cooperative Travelers Assistance (CTA): This application focuses on assistance of the drivers. It increases the transparency of the evolving traffic situation downstream on the road network, personalizes the information to travelers, enables them to make optimal use of the road network and assists the traveler making the right choice navigating through the road network, based upon full cooperation between Roadside systems, in-vehicle sensors, Traffic managers

and Service providers. This system will provide information to the driver within 15 seconds about a major congestion incident, and 15 seconds later they receive a recommendation about an alternative route.

3. *CF&F - Cooperative Freight & Fleet*: aims to increase the safety of dangerous goods transport and optimize transport companies' delivery logistics. The aim is to develop innovative co-operative systems for commercial vehicles where information about the current positions, the cargo types and the destinations of freight transport vehicles are given to the regional public authorities in order to increase: efficiency, safety, security, and environmentally friendliness of cargo movements. The cooperation approach will be shown in three different application areas: (i) monitoring and guidance of dangerous goods, (ii) parking zone management, and (iii) access control to sensitive infrastructures. The driver can have more precise and up-to-date information on: local traffic conditions and regulations/limitations affecting his journey, available parking zones for goods loading/unloading and resting, and suitable routes for the specific goods being transported.

To provide these cooperative applications with monitoring data anywhere and at any time, CVIS project defines a Cooperative Monitoring (COMO) block. It is placed as a central basic service inside the CVIS framework and will cooperate closely with CURB, CINT and CF&F applications to capture their particular requirements about monitoring of traffic and environmental information. The high data volume generated by fixed and mobile sensors requires new, innovative approaches to achieve fast response times and a reasonably (in-)expensive data communication between the vehicles, the roadside units and the centers. Since fully centralized systems might not be able to serve all of these goals, the aim is a cooperative system environment in which COMO is implementing applications for data collection, data fusion and (potentially) other applications. Hence, COMO aims to develop specifications and prototypes for the collection, integration and delivery of extended real-time information on individual and collective vehicle movements and on the state of the road network.

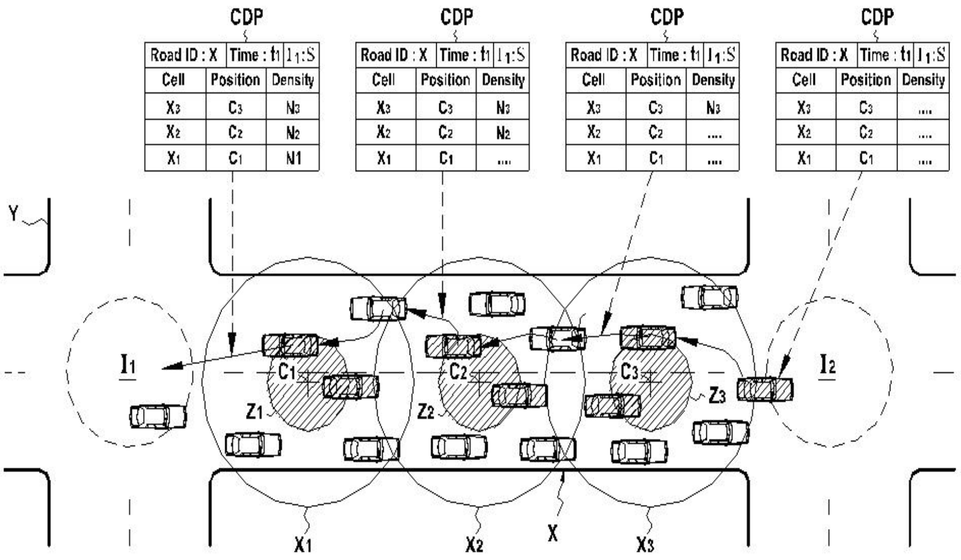
Particularly appealing examples that will use this cooperative monitoring block are IFTIS [38] and the parking zone management SmartPark [39]. IFTIS is a completely distributed and infrastructure-free mechanism for road density estimation. IFTIS is based on a distributed exchange and maintenance of traffic information between cooperating vehicles traversing the routes. It provides cooperative urban applications with real time information about the traffic within city roads. The idea of SmartPark is to solve the parking problem in a completely cooperative and decentralized fashion.

In the following, we give details of some of these applications and quantify performance gains due to relaying and cooperation.

3.4.1 Traffic Density Estimation

One of the most important components of the Intelligent Transportation System is the road traffic information handling (monitoring, transmission, processing and communication). The existing traditional ITS traffic information systems are based on a centralized structure in which sensors and cameras along the roadside *monitor* traffic density and *transmit* the result to a central unit for further *processing*. The results will then be *communicated* to road users via broadcast service or alternatively on demand via cellular phones. The centralized approaches are dependent on fixed infrastructures which demand public investments from government agencies or other relevant operators to build, maintain, and manage such infrastructure: a large number of sensors are needed to be deployed in order to monitor the traffic situation. The traffic information service is then limited to streets where sensors are integrated. Besides, centralized designs have the disadvantage of being rigid, difficult to maintain and upgrade, require substantial computing/communications capabilities, and are susceptible to catastrophic events (sabotage or system failures). Moreover, such systems are characterized by long reaction times and thus are not useable by all the applications requiring reliable decision making based on accurate and prompt road traffic awareness.

We proposed a completely decentralized mechanism for the estimation of vehicular traffic density in city-roads IFTS (Infrastructure-Free Traffic Information System) [38]. The decentralized approach is based on the traffic information exchanged, updated and maintained among vehicles in the roads and revolves around the core idea of information relaying between groups of vehicles rather than individual vehicles. More precisely, the vehicles are arranged into location-based groups. For that, each road (section of street between two intersections) is dissected into small fixed area cells, each defining a group. Note that the cell size depends on the transmission range of vehicles and the coordinates of the cell center gives the cell a unique identifier. Cells, and hence groups, overlap in such a way that any vehicle moving from one cell to the next belongs at least to one group. Among vehicles within the zone leader[2], the closest vehicle to the cell center is considered as the group leader for a given duration. Note that the overlapping zone is so small that it is not possible that a vehicle is considered to be group leader of both adjacent cells.



Road ID : X	Time : t1	I1:S
Cell	Position	Density
X3	C3	N3
X2	C2	N2
X1	C1	N1

Road ID : X	Time : t1	I1:S
Cell	Position	Density
X3	C3	N3
X2	C2	N2
X1	C1	....

Road ID : X	Time : t1	I1:S
Cell	Position	Density
X3	C3	N3
X2	C2	....
X1	C1	....

Road ID : X	Time : t1	I1:S
Cell	Position	Density
X3	C3	....
X2	C2	....
X1	C1	....

Figure 4. Relaying local density information between groups.

Local density information is then computed by each group leader and relayed between groups using Cell Density Packet (CDP). The CDP gathers the density[3] of a given road (i.e., all its cells). When initiating the CDP, a vehicle records the road ID, the transmission time[4] and a list of anchors through which the packet has to pass while travelling to the other intersection, and then, sends the packet in the backward direction. The CDP header includes a limited list of anchors corresponding to the position of the cells' centers. Then, the CDP is forwarded towards the first anchor on the basis of greedy forwarding. Once the message is received by a group leader (the closest vehicle to the cell center), this later updates it by including the density of the corresponding cell (the number of its neighbors) and then forwards it towards the next anchor. This is repeated until the CDP is completed while arriving to the destination intersection. After the last anchor (the destination intersection) is reached, the CDP is propagated to vehicles which are around the intersection so that all vehicles traversing through the intersection will receive it. These vehicles analyze the packet content and calculate the density for the respective road from which the CDP was received. This analysis is done by computing (i) the average number of vehicles per cell N_{avg} and (ii) the standard deviation of cells densities σ. Note that the standard deviation indicates how much variation there is away from the N_{avg}: a large standard deviation indicates that the cells densities are far from the mean and a small standard deviation indicates that they are clustered closely around the mean.

The performance analysis of the proposed mechanism depicted the accuracy of IFTIS and the promptness of information delivery based on delay analysis at the road traffic intersections. This is done in a distributed manner and based only on the cooperation between vehicles.

3.4.2 Smart Parking

The main goal of SmartPark [39] is to collect information about parking space availability and to coordinate drivers in order to guide them to free parking spots. To this extend, at every parking spot a wireless mote is deployed which tracks the occupancy and cooperates with other nearby motes and vehicles. Each vehicle is equipped with a wireless

[2] A small area around a cell center where a vehicle is elected as a group leader.
[3] By density, we mean the number of vehicles within the cell.
[4] Note that all the vehicles are synchronized by GPS.

communication device that provides a driver with information about parking space availability and guides them eventually by turn-by-turn instructions.

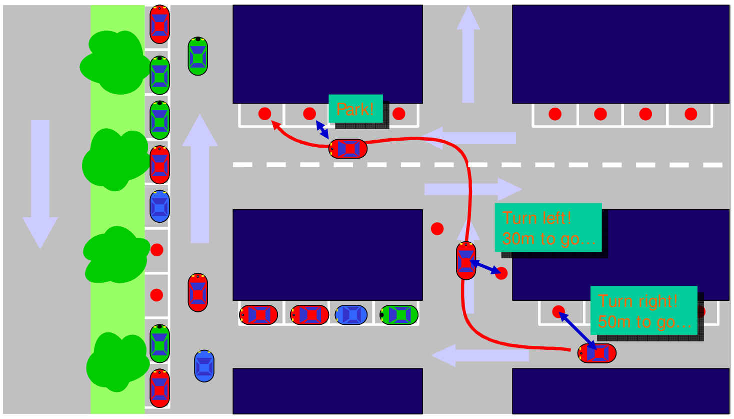


Figure 5. SmartPark system consists of sensor nodes embedded in parking spaces and on-board units inside vehicles.

4. Conclusion

Thanks to the advances in wireless technologies, vehicular networks have been emerged as a new type of autonomous networks allowing for vehicle-to-infrastructure and vehicle-to-vehicle communication. Applications in vehicular networks range from road safety applications oriented to the vehicle or to the driver, to entertainment and commercial applications for passengers, making use of a plethora of cooperating technologies. Passing traffic information such as travel times or warning messages about accidents or sloppy roads are only a few examples of the potentials created by equipping vehicles and roads with appropriate communication capabilities. The increased number of vehicles on the road increases significantly the unpredictable events outside vehicles. In fact, accidents arrive rarely from vehicles themselves and mainly originate from on-road dynamics. This means that cooperation using vehicular networks must be introduced into transportation networks to improve overall safety and network efficiency, and to reduce the environmental impact of road transport. Moreover, cooperation is crucial in entertainment applications to allow reliable services’ access through the multihop communication during vehicles’ mobility.

Cooperative techniques will likely survive in scenarios which are independent of users (no selfishness) but rather depending on machines or operator-programmed decision engines. Examples are machine-to-machine applications, such as vehicular networks In this chapter we explored cooperation issues in autonomous vehicular networks at different levels. We notice that high-level services should be build following a cooperative model that depends exclusively on the participation of contributing vehicles and the existing infrastructure. We also notice that vehicular networks scenarios relying on an infrastructure (that could be eventually limited infrastructure) could satisfy cooperation through resolving several technological issues. Such scenarios are promising for real deployment of vehicular networks in a public context of generalized mobility.

5. References

[1] J. Blum, A. Eskandarian and L. Hoffmman, “Challenges of intervehicle ad hoc networks” *IEEE Transactions on Intelligent Transportation Systems*, Vol. 5, No 4, pp. 347-351, 2004.

[2] M. Dohler, D.-E. Meddour, S.-M. Senouci, H. Moustafa, "Cooperative Communication System Architectures for Cellular Networks" *in M. Uysal (Edt)* "Cooperative Communications for Improved Wireless Network Transmission: Frameworks for Virtual Antenna Array Applications," *IGI-Global*, ISBN: 978-1-60566-665-5, July 2009.

[3] T. Taleb, Z. Fadlullah, A. Benslimane, and K. Ben Letaief, “Towards an Effective Risk-conscious and Collaborative Vehicular Collision Avoidance System," accepted in IEEE Tran. Vehicular Technology.

[4] G. M. T. Abdalla, M. Ali Abu -Rgheff, SM. Senouci, "Space -Orthogonal Frequency -Time Medium Access Control (SOFT MAC) for VANET", *IEEE GIIS'2009*, Hammamet, Tunisia, June 23-25, 2009.

[5] M. Jerbi, SM. Senouci, T.M. Rasheed, Y. Ghamri-Doudane, "Towards Efficient Geographic Routing in Urban Vehicular Networks," *IEEE Transactions on Vehicular Technology*, to appear in 2009.

[6] M. Jerbi, SM. Senouci, R. Meraihi and Y. Ghamri-Doudane, "An Improved Vehicular Ad Hoc Routing Protocol for City Environments", *IEEE ICC'2007*, Glasgow, Scotland, UK, 24-28 June 2007.

[7] M. Cherif, SM. Senouci, and B. Ducourthial, "Vehicular Network Self-Organizing Architectures", *IEEE GCC'2009*, Kuwait, March 17-19, 2009.

[8] I. Salhi, SM. Senouci, and M. Cherif, "A New Framework for Data Collection in Vehicular Networks", *IEEE ICC'2009*, Dresden, Germany, June 14-18, 2009.

[9] A. Benslimane, "Optimized Dissemination of Alarm Messages in vehicular ad-hoc networks (VANET)", HSNMC, 2004, LNCS 3079, pages 655–666.

[10] Tamer ElBatt, et al., "Cooperative Collision Warning Using Dedicated Short Range Wireless Communications", *VANET'06,* September 29, 2006, Los Angeles, California, USA.

[11] R. Tatchikou, et al., "Cooperative vehicle collision avoidance using inter-vehicle packet forwarding", Globecom 2005, pp. 2762-2766.

[12] Yao H. Ho, et al., "Cooperation Enforcement in Vehicular Networks", Conference on Communication Theory, Reliability, and Quality of Service (CTRQ), 2008, pp. 7-12.

[13] X. Yang, et al., " A Vehicle-to-Vehicle Communication Protocol for Cooperative Collision Warning ", Mobiquitous 2004, pp.114-123.

[14] C. Bettstetter, H. Adam, SM. Senouci, "A Multi-Hop-Aware Cooperative Relaying", *IEEE VTC'2009 Spring*, Barcelona, Spain, 26–29 April.

[15] H. Adam, C. Bettstetter, SM. Senouci, "Adaptive Relay Selection in Cooperative Wireless Networks", *IEEE PIMRC2008*, Cannes, France, 15-18 September 2008.

[16] G. Korkmaz, E. Ekici and F. Özgüner, "Urban multihop broadcast protocol for inter-vehicle communication systems", *IEEE Transactions on Vehicular Technology*, Vol. 55, No. 3, pp. 865-875, 2006.

[17] H. Wu, R. Fujimoto, R. Guensler, and M. Hunter, "MDDV: a mobility centric data dissemination algorithm for vehicular networks", *In Proceedings of the 1st ACM Workshop on Vehicular Ad Hoc Networks (VANET'04)*, Philadelphia, PA, USA, Sep. 2004.

[18] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks" *In Proceedings of the 6th ACM/IEEE International Annual Conference on Mobile Computing and Networking (MOBICOM'00)*, Boston, MA, USA, August 2000.

[19] D. Niculescu and B. Nath, "Trajectory based forwarding and its applications" *In Proceedings of the 9th ACM International Annual Conference on Mobile Computing and Networking (MOBICOM'03)*, San Diego, USA, 2003.

[20] C. Lochert, H. Hartenstein, J. Tian, D. Herrmann, H. Füßler, M. Mauve, "A Routing Strategy for Vehicular Ad Hoc Networks in City Environments" *In Proceedings of IEEE Intelligent Vehicles Symposium (IV'03)*, Columbus, OH, USA, Jun. 2003.

[21] B.-C. Seet, G. Liu, B.-S. Lee, C. H. Foh, K. J. Wong, K.-K. Lee, "A-STAR: A Mobile Ad Hoc Routing Strategy for Metropolis Vehicular Communications" *In Proceedings of the 3rd IFIP International Conferences on Networking (NETWORKING'04)*, Athens, Greece, May, 2004.

[22] J. Zhao and G. Cao, "VADD: Vehicle-assisted data delivery in vehicular ad hoc networks" *IEEE Transactions on Vehicular Technology*, Vol. 57, No. 3, May. 2008.

[23] J. Davis, A. Fagg, and B. Levine, "Wearable Computers as Packet Transport Mechanisms in Highly-Partitioned Ad-Hoc Networks" *in Proceedings of the 5th International Symposium on Wearable Computing (ISWC'01)*, Zurich, Switzerland, Oct. 2001.

[24] J. Nzoonta and C. Borcea, STEID: A protocol for emergency information dissemination in vehicular networks, Draft, 2006.

[25] G. Korkmaz, E. Ekici, F. Özgüner, and Ü. Özgüner, "Urban multihop broadcast protocol for inter-vehicle communication systems," in VANET '04: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks. Philadelphia, PA, USA: ACM Press, Sept. 2004, pp. 76–85.

[26] M. Jerbi, SM. Senouci, AL. Beylot, Y. Ghamri, “Geo-localized Virtual Infrastructure for VANETs: Design and Analysis”, *IEEE Globecom 2008*, New Orleans, LA, USA, 30 November - 4 December 2008.

[27] R.H. Frenkiel, B.R. Badrinath, J. Borras, and R. Yates, “The Infostations Challenge: Balancing Cost and Uiquity in Delivering Wireless Data,” in IEEE Personal Communications, April 2000.

[28] B. Liang and Z.J. Haas, "Virtual backbone generation and maintenance in ad hoc network mobility management", *IEEE INFOCOM 2000*, pp.1293-1302, Tel-Aviv, Israel, March 2000.

[29] B. Chen, K. Jamieson, H. Balakrishnan and R. Morris, "Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks", *ACM Wireless Networks Journal*, vol.8, n°5, pp.481-494, September 2002.

[30] H. Moustafa, G. Bourdon and Y. Gourhant, “Authentication, authorization, and accounting (AAA) in hybrid ad hoc hotspots’ environments,” ACM WMASH, 2006.

[31] H. Moustafa, J. Forestier and M. Chaari, “Distributed Authentication for Services Commercialization in Ad hoc Networks,” ACM Mobility Conference 2009.

[32] D. Forsberg, O. Ohba, B. Patil, H. Tschofenig, and A. Yegin, “Protocol for carrying authentication and network access (PANA),“. RFC 5193, May 2008.

[33] S. Marti, T. J. Giuli, K. Lai, and M. Baker, ”Mitigating routing misbehavior in mobile ad hoc Networks,” ACM Mobicom, 2000.

[34] S. Buchegger, and J. Y. le Boudec, “Performance analysis of the CONFIDANT protocol,” ACM MobiHoc, 2002.

[35] R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan, “Sustaining cooperation in multihop wireless networks,” ACM NSDI, 2005.

[36] M. Raya, J. P. Hubaux, and I. Aad, “Domino: A system to detect greedy behavior in IEEE 802.11 Hotspots,“ ACM MobiSys 2004.

[37] CVIS project, http://www.cvisproject.org/

[38] M. Jerbi, SM. Senouci, T. Rasheed, Y. Ghamri-Doudane, "An Infrastructure-Free Traffic Information System for Vehicular Networks", *IEEE WiVeC 2007*, Baltimore, USA, 30 September - 1 October 2007.

[39] SmartPark, http://smartpark.epfl.ch/

[40] S. Barghi, A. Benslimane and C. Assi, **“**Connecting Vehicular Networks to the Internet : A Life Time-based Routing Protocol”, *10th IEEE International Symposium World of Wireless, Mobile and Multimedia Networks & Workshops (WoWMoM 2009)*, Kos Greece, pp.1 – 9, 15-19 June 2009.