Routing in Vehicular Networks: Feasibility, Security and Modeling Issues

Ioannis Broustis and Michalis Faloutsos
Department of Computer Science and Engineering
University of California, Riverside
Riverside, CA, 92521
{*broustis, michalis*}*@cs.ucr.edu*

***Abstract*— Vehicular networks are sets of surface transportation systems that have the ability to communicate with each other. There are several possible network architectures to organize their in-vehicle computing systems. Potential schemes may include vehicle-to-vehicle ad-hoc networks, wired backbone with wireless last-hops, or hybrid architectures using vehicle-to-vehicle communications to augment roadside communication infrastructures. Some special properties of these networks, such as high mobility, network partitioning and constrained topology, differentiate them from other types of wireless networks. In this article we revisit most of the important studies on designing architectures and discussing routing aspects for such networks. Moreover, we provide the basic concepts of traffic flow theory and we discuss the major security concerns appearing in vehicular networks.**

***Index Terms*—Wireless Communication, Ad Hoc Vehicular Networks (VANETs), Modeling, Network Topology, Security.**

I. Introduction

Vehicular computing systems allow the potential set-up of vehicular networks in all kinds of environments. The FCC has allocated 75 MHz of spectrum at 5.9 GHz for short-range communications between vehicles and from vehicles to roadside facilities. Such networks offer the potential for fast and accurate driving information (e.g. traffic, accidents and emissions) that would otherwise be more difficult to disseminate. Hence, new ways to improve and optimize the transportation system are enabled. Also a variety of commercial applications can easily be supported. Vehicular networks can be used to facilitate the service customization to the needs of individual nodes. Possible applications for such networks can be generally classified as safety and non-safety applications. Safety applications include accident avoidance and cooperative driving [1]. Non-safety applications include traffic information [2], toll service, Internet access [3], cooperative entertainment, etc.

Vehicular networks consist of nodes - vehicles equipped with wireless communication devices, GPS, digital maps and optional sensors for reporting the vehicle condition. Vehicles exchange information with other vehicles as well as with access points (base stations) within their radio range. Ad hoc or infrastructure wireless networks are used to propagate information. However, the data propagation requires innovative routing algorithms. This is because, as we explain later, vehicular networks have unique characteristics that differentiate them from common wireless networks. As a consequence, routing is a challenging task, due to the high dynamics of such a network.

In this article we investigate: *(1)* The extent to which the vehicular network characteristics can determine the performance of routing. *(2)* How can current wireless technologies (e.g. WiFi, UWB,WiMax, cellular) support vehicular networks. *(3)* Most of the important related studies on vehicular network architectures and routing. We do not focus specifically on one type of architecture; in contrast we describe and comment on most currently famous suggested schemes. *(4)* Finally, how feasible is to maintain a level of security in such networks.

The remainder of this article is organized as follows. In section II, we discuss the unique characteristics of vehicular networks, and how these demand innovative routing protocols. In section III we provide a small analysis, deriving some vehicular network metrics, essential for creating vehicular movement models. Moreover, in section IV we present related studies on vehicular network routing. We also add our comments about the validity and the importance of them. Some routing and topological security concerns are mentioned in section V. Specifically we discuss how can the vehicular network properties affect the impact of malicious attacks, as well as some general miti-

gation schemes. Finally, section VI concludes this paper.

II. Background

A. *Vehicular Network Properties*

As we mentioned earlier, vehicular networks have specific characteristics. These properties affect the decisions that designers have to take, when building architectures for such networks. This is because some of their characteristics, prohibit the use of current routing protocols that are applicable to regular wireless networks. Here we discuss these uniquenesses.

a) Geographically constrained topology: Roads limit the network topology to actually one dimension; the road direction. Except for crossroads or overlay bridges, roads are generally located far apart. Even in urban areas, where they are located close to each other, there exist obstacles, such as buildings and advertisement walls, which prevent wireless signals from traveling between roads. This implies that nodes-vehicles can be considered as points of the same line; a road can be approximated as a straight line, or a small-angled curve. This observation is quite important, because it affects the wireless technologies that can be considered. For example, since the packet relays are almost all in the same one-directional deployment region, the use of directional antennas could be of great advantage.

b) Partitioning and large-scale: In vehicular networks, the probability of end-to-end connectivity decreases with distance [5]; this is true for one-dimensional network topologies. In contrast, connectivity is often explicitly assumed in research for traditional ad hoc networks, sometimes even for the evaluation of routing protocols. In addition, vehicular networks can extend in large areas, as far as there is road available. This artifact together with the one-dimensional deployment increase the above probability.

c) Predictable mobility: Because vehicle mobility depends on the deployment scenario, the movement direction is predictable to some extent. In highways, vehicles often move at high speeds, while in urban areas they are slow. In addition, mobility is restricted by the road directions as well as by traffic regulations. Assuming that these regulations are obeyed, there are lower and upper speed bounds, and restriction signs that obligate drivers to move on specific roads and directions. Hence, mobility models can now include some level of predictability in movement patterns. Car manufacturing companies have already implemented such models for testing mechanical parts.

d) Power consumption: In traditional wireless networks, nodes are power limited and their life depends on their batteries - this is especially true for ad hoc networks. Vehicles however can provide continuous power to their computing and communication devices. As a result, routing protocols do not have to account for methodologies that try to prolong the battery life. Older network protocols include mechanisms such as battery-life reports for energy-efficient path selection, sleep-awake intervals, as well as advanced network/MAC cross-layer coordination algorithms. These schemes cannot offer any additional advantages to vehicular networks.

e) Node reliability: Vehicles may join and leave the network at any time and much more frequently than in other wireless networks. The arrival/departure rate depends on their speed, the environment, as well as on the drivers' needs to be connected to the network. Especially for ad hoc deployments, the network cannot easily depend on a single vehicle for packet forwarding. This is because the duration of the vehicle's cooperation depends on its destination. Also, apart from vehicles failing in unpredictable ways, security issues come into play. We discuss these issues later in this article.

B. *Potentially Applicable Wireless Technologies*

There are three potential wireless technologies under discussion that can be adopted: Wireless Metropolitan Area Networks (WMANs), Wireless Local Area Networks (WLANs/WiFi) and Wireless Personal Area Networks (WPANs), together with their ad hoc mode of operation.

a) WMANs: A WMAN *(Wireless Metropolitan Area Network)* can interconnect distant locations. Two kinds of WMANs exist: back haul and last mile. Back haul is for enterprise networks, cellular base station communications and Wi-Fi hotspots. A private WMAN broadband system is a quite chip solution and it is 10 times faster than a DSL or T1 wireline connection. Thus, it is affordable for companies that do not wish to pay double the price for a fiber 10-MBps link to their ISPs. Last-mile setups can establish wireless as an alternative to residential broadband modems. In a typical cell radius deployment of three to ten kilometers, last mile systems can be expected to deliver capacity of up to 40 Mbps per channel. This is enough bandwidth to simultaneously support hundreds of businesses with T1 speed connectivity and thousands of residences with DSL speed connectivity.

WMAN connections can be PTP (Point-To-Point) or PMP (Point-To-Multipoint). Both omnidirectional and directional antennas can be used, as well as dynamically alternated radio channels and antenna polarization. PMP

set-ups, where a central point serves multiple remote sites, are preferable when the density of links is high. PMP systems typically use a polling protocol to support high-density applications. One of the most interesting recent developments is the standardization of WMANs in the form of IEEE 802.16. Finally, the WMAN category also includes the GSM/GPRS Cellular infrastructure networks.

The WMAN type of technology could be employed in infrastructure-based vehicular networks alone, or in coordination with WLANs or WPANs (and their ad hoc multihop types) as last-hops. *WiMax* promises to bring wireless high-speed connections to entire metropolitan areas. It is currently supported by 140 companies. WiMax has a reach of 1 to 10 miles, offering a way to bring the Internet to entire communities. Mobile network deployments are expected to provide up to 15 Mbps of capacity within a typical cell radius deployment of up to 3 kilometers. This is an obviously high-potential solution for vehicular networks, even for distant highway environments.

When collaborating with WiFi/WPANs, the WMAN may provide the permanent connectivity. The PAN/WiFi portion could be added from the base stations to the vehicles, as well as among vehicles themselves[1], to offer high bandwidth with low cost. Also, a potential protocol could support the direct connectivity of a vehicle with the WMAN, either when there is lack of a WLAN base station in that area, or when the number of hops to the base station exceeds some threshold. An alternative could also be to maintain permanent direct links from vehicles to cellular base stations, without the direct communication among vehicles. However, from the cellular network perspective this will probably result in a relatively low throughput. Currently the GSM/GPRS technology ideally offers at most 100 KBps of bandwidth. Also 3G systems can reach 384 KBps. Future cellular PHY technologies may provide higher throughputs, allowing more data rate-demanding applications to be supported.

b) WLAN/WiFi: WiFi is another possibility for vehicular networks. An IEEE 802.11 transmitter has a 250-meter omnidirectional coverage range, which is potentially enough to maintain a level of multihop connectivity in both highway and urban regions. In addition, extended-vicinity antennas (umbrellas) could be employed in base stations, for covering larger distances. A lot of research has been done for the popular IEEE 802.11 wireless protocol, mostly for the MAC (CSMA/CA) and network layers. However, this research cannot be taken ”off the shelf” for use in vehicular networks. This is because of the unique properties that we described above.

[1]V2V (Vehicle-To-Vehicle multihop communications)

c) WPAN: Wireless Personal Area Networks are used for short-range wireless communications. Two of the most popular technologies, Bluetooth and Ultra Wide Band (UWB) belong to this category. While the former offers a low data rate (up to 10 MBps for Bluetooth v2.0), the latter promises very high data rates, up to 500 MBps. Even though there has been a lot of work done for the PHY layer or UWB, concerning modulation and channelization, only a few studies exist for upper layers. Especially for UWB ad hoc networks, MAC and network layer protocols are still under consideration and no standards exist for them. Even though the data rates offered by UWB are tempting, the short transmission range (maximum 10-20m) restricts the applicability of this technology to only dense urban-area vehicular networks.

In summary, we believe that the most appropriate wireless technology for vehicular networks is the WMAN technology alone, or WMAN in cooperation with WiFi and sometimes with WPANs. We argue that the cellular technology is rather useless for these networks, especially in cases or delay-sensitive applications; delay-tolerant applications could be addressed. The high mobility as well as the network partitioning and scalability demand the employment of either infrastructure-based wireless infrastructures or scalable ad hoc solutions, such as hierarchical clustering structures, etc.

C. *Applications*

Applications running on top of vehicular networks can be categorized as safety and non-safety applications: driver-vehicle safety, infotainment, and mobile internet services for passengers. In addition to low cost and robust wireless communication devices, vehicles can also be equipped with storage, processing and sensing capability. Vehicles can be used as store-and-forward mobile routers, on-demand and dynamic grid computing engines, as well as distributed mobile sensor networks.

There are a number of projects, completed or under development, targeting to improve roadway conditions. Fleenet [3], funded by the German Federal Ministry for Education and Research, focuses on mobile ad hoc radio networks. Fleenet applications include emergency braking notification and traffic data distribution. The VMesh/VGrid project [17] has two directions. In *VMesh*, vehicles dynamically form a mobile transit network to gather and dessiminate information. For example, data may be relayed between different clusters of static nodes that are otherwise disconnected. *VGrid* targets to evolve intelligent transportation system *(ITS)* from a centralized to a distributed approach, in which vehicles can cooper-

atively solve traffic-flow control problems. Furthermore, one of the most intelligent transportation systems exists in Singapore. It includes real-time surveillance of road speeds, road pricing, advanced traffic signal control and an advanced mass transit system. Near-future "smart" *vehicular computational devices* of various types will be able to communicate with each other and utilize their diverse resources: wireless networks, embedded processors and sensors, databases, satellites, etc. This implies the need for innovative communication protocols, specialized to adopt the unique properties of vehicular networks and the availability of their resources.

An interestings information architecture toolkit is discussed in [13]. It includes (1) wireless networking capabilities, (2) traffic prediction algorithms, (3) vehicle and trajectory recognition based on fusing heterogeneous data, (4) cost models (fairness, robustness, privacy, computational efficiency), and (5) real-time maintenance, prediction and generation of spatiotemporal information. The kit can be used in a variety of applications: planning multi-modal routes, exchange of real-time traffic information, autonomous - unmanned vehicle driving and, of course, multi-vehicle cooperation *(MVEC)*. For this latter application, vehicles are assumed to be equipped with GPS receivers, computational devices and wireless communication systems. Vehicles will be able to process queries, such as *"what is the average vehicle speed 2 miles ahead?"*. Processing such queries demands multihop links and mobile-database utilization.

III. Vehicular Flow Theory

As we mentioned earlier, vehicles are characterized by high and predictable mobility and such networks usually have an one-dimensional topology. Thus, understanding the basic concepts of traffic flow theory [7] is crucial for designing routing protocols and evaluating their efficiency.

Most of the models used to reproduce or simulate vehicle movement employ three basic mobility concepts: speed u, density k and flow q. For the purposes of this small analysis, the notion of lane occupancy L must be defined. We define S_{veh} to be the sum of vehicle lengths along a road region, and S_r to be the length of this road region. We then have:

$$L = \frac{S_{veh}}{S_r} \tag{1}$$

We can then compute the vehicular density k as:

$$k = \frac{L}{S_{veh-average}} \tag{2}$$

The acute reader can understand that, with few vehicles the density tends to zero, while as more vehicles come on the road, the density increases. However, in the above equation we cannot approximate the value of S_{veh} with online methods. Thus, time measurements are used to estimate L. These measurements take place on the road using magnetometers, ultrasonic reflectors and photo cells. One may then count the number of vehicles crossing the measurement spot, as well as the time t_r that the reflector is reacting. The number of nodes during the observation period T is then calculated as:

$$N = \frac{t_r}{T} \tag{3}$$

Using satellite images one can also compute the number of nodes N on a road region of length S_r. Then density is easily computed as:

$$k = \frac{N}{S_r} \tag{4}$$

Moreover, the average vehicular speed can also be determined from satellite images. This is if a number of such images are taken sequentially with a small interval among them. Another way of measuring the above values, as well as the flow is the moving observer procedure. An observer first travels in the same direction as the traffic flow and then returns in the opposite direction., measuring the the travel time. During these travels, the number of vehicles is measured. More specifically, while moving in the flow's direction the observer counts the number of vehicles that pass its vehicle. For the travel in the opposite direction the number of encountered vehicles are counted. We then define:

1) t_c the travel time with the flow
2) t_a the travel time against the flow
3) x number of vehicles counted while moving with the flow
4) y number of vehicles counted while moving against the flow

Having measured the above values, we may further calculate the flow as:

$$q = \frac{x + y}{t_a + t_c} \tag{5}$$

In addition, the speed is computed from the following equation:

$$u = \frac{S_{veh}}{t_c - y/q} \tag{6}$$

And finally, the measured density will be:

$$k = \frac{q}{u} \tag{7}$$

Furthermore, some models employ another method to calculate the flow. According to this method, the observer counts the number x of vehicles passing in the opposite direction (of the flow). If v_1 is the speed on oncoming vehicles and v_0 is the observer's speed, then the flow is given from the following:

$$q = \frac{x}{S_{veh}\dot{(}\frac{1}{v_1} + \frac{1}{v_0})} \quad (8)$$

As we said previously in this section, the models used to simulate vehicular movement need to adopt basic properties, derived from traffic flow theory. Selecting and calculating the appropriate metrics helps in evaluating correctly the impact of vehicular mobility to network performance.

IV. Related Studies on Vehicular Routing

There has been a lot of interest to exploit the potentials of vehicular networks. However only a few studies propose complete routing solutions and architectures. In this section we present the most important of these studies. We may have various categorizations for them. One could be to separate them according to the type of architecture that they import: ad hoc or infrastructure or hybrid. Another categorization could involve the deployment region: highway or urban regions. Below we describe and discuss the most important ones.

Most studies in vehicular routing focus either on comparing current routing solutions for traditional wireless networks, or describing issues that must be taken into account, when building appropriate models. In [11] Mauve et al. examine the applicability of existing ad hoc routing protocols to VANETs. Specifically, they compare the famous Dynamic Source Routing (DSR) and the Greedy Perimeter Stateless Routing (GPSR) protocols. They conclude that when communication sessions are comprised or more than 2 or 3 hops, position-based ad hoc routing is preferable over reactive non-position-based approaches. The advantages have to do with both the successfully delivered packets and the control overhead. In addition, the authors argue that the random waypoint model is rather inappropriate to accurately reproduce vehicle movement. Alternatively they make use of the well-validated FARSI simulator, adopted by many car companies to generate traffic simulation scenarios. For their simulations they assume the deployment of the IEEE 802.11 protocol. They show that current position-based schemes provide high data rates, even over many hops. Moreover, the overhead is small and does not impact on scalability. The reason is that position-based routing does not store routes and instead performs forwarding on the fly. An improvement to DSR could involve considering the movement of individual vehicles in the routing decision. Thus, preference to routes over vehicles moving in the same direction can be given. As a result, topological changes would be infrequent. Finally, for position-based schemes, they generally propose caching and prediction of a node's location, based on its speed and direction.

MDDV: The Mobility-Centric Data Dissemination Algorithm *(MDDV)* [6] is one of the few that provide a complete architecture for vehicular routing. It combines the ideas of opportunistic forwarding, trajectory-based forwarding and geographical forwarding. The protocol disseminates data to intended receivers, while maintaining some design demands, e.g. high delivery ratio, low delay and low memory occupancy. Even though MDDV can be applied to hybrid architectures, it is considered in VANET scenarios only.

A *forwarding trajectory* is a predefined path, extending from the source to the destination region. Moreover, the road network can be thought of as a directed graph, with nodes representing intersections and edges being the road segments. One approach would consider taking the shortest (road) graph distance from the source to the destination region. However this does not imply the lowest delay, since node density often leads to fast propagation. Thus, the authors define as:

1) $d(A, B)$ the dissemination length of the road segment from node A to node B, considering static road information.
2) $r(A, B)$ the road length from A to B. Intuitively, when j=0 and i=1 we have $d(A, B)$=$r(A, B)$
3) i/j the number of lanes from A/B to B/A.

For the dissemination length, the following formula is used:

$$d(A, B) = r(A, B)(m - (m - 1)(i^p + cj^p)) \quad (9)$$

The constants p and c take values between 0 and 1. Constant m is set to 5.

The dissemination length is used as weight for the corresponding link in the graph. The dissemination process has two phases: the forwarding phase and the propagation phase, described below. Because no end-to-end connectivity is assumed, messages are forwarded along the forwarding trajectory through intermediate nodes; these store and forward messages opportunistically. The vehicle that holds the message and is the closest one to the destination region is called the *message head*. To increase reliability, MDDV allows a set of nodes near the message head to ac-

tively forward the message, instead of the message head alone. However this also implies overhead increment. The design issues include the forwarding group identification, the data exchange procedure and the decision to store/drop messages. Each node decides whether it will participate in forwarding or not, based on the traffic information in the area, as well as with some approximate knowledge of the message head location. The message head location never moves backward; a new message head location is closer to the destination than previous ones. In a nut shell, the data exchange steps are the following:

a) Forwarding phase: The message to be sent is assigned an owner. Usually the owner is the same as the head. Only the message owner may transmit the certain message, and the owner can be in either one among two states: active or passive. In the active state it runs the full protocol to actively propagate the message. In the passive state it only transmits the message if it hears an older version of it.

b) Propagation phase: It is initiated once the message reaches the destination region. The message now further propagates to each vehicle in the area centered at the destination, before the message time expires. In this phase, the message owner can either be in the active state, or not transmitting at all. During this phase the message is delivered to its recipient(s).

The paper provides a more detailed explanation of the algorithm, which we avoid reproducing here. It also present the scheme in only one forwarding trajectory. However, multiple of them could be defined, to increase robustness. Also, simulation results show the improved efficiency with regards to two simple schemes.

GSR: In [4] the Geographic Source Routing protocol is proposed. [4] examines the problems appearing with base-line position-based routing in *two-dimensional* urban scenarios. GSR combines position-based routing with topological information.

The adoption of the RLS [18] system is assumed. The source uses flooding to request the position of a node identifier. As soon as that node receives the request, it sends a position response back to the source. After discovering the location of the recipient, the source uses a digital map of the roads to calculate the set of junctions that the packet will follow. This set can be either imported to the packet header, or be derived by every forwarding node. This latter approach can be implemented on the basis of greedy forwarding. The paper discovers the source-destination route through the Dijkstra algorithm. An issue arises from the fact that the paper compares GSR with non-position-based protocols only. There is no comparison with other position-based schemes, such as GPSR, proposed 3 years earlier.

A-STAR: Lee et al. in [10] present *A-STAR*, an Anchor-based Street and Traffic Aware Routing scheme. They use information on city bus routes to identify an anchor path with high connectivity for packet delivery. The model is designed based on position-based routing, specifically to facilitate VANETs in urban areas. In such environments, vehicle density is larger in some *famous* (for their traffic) roads than in others. Connectivity is such roads can be higher and more stable, due to regular bus passes. Also buildings constrain the signal propagation. Hence, it is more difficult to establish wireless connectivity in urban areas - the network efficiency is decreased.

A-STAR constructs a graph, based on how many bus lines go through certain roads. The number of lines determines the link weight for the certain edge of the graph. The more the routes, the less the weight. Since each vehicle may be aware of the bus route information through digital maps, an *anchor* route may be constructed using the Dijkstra's algorithm for least-weight. Maps with preconfigured routes are called statically rated maps. In contrast, a dynamically rated one can be utilized. In such a digital map, weight assignment is performed dynamically, by periodically monitoring the street traffic and updating the graph weights. Message propagation from the source to the destination follows the route produced by Dijkstra's algorithm.

The protocol includes its own local route recovery. The local recovery mechanisms adopted by other protocols, have been proven to be inefficient in urban areas, because of the greedy-forwarding phase. To solve this problem, A-STAR discovers new anchor paths from the *local maximum* to which the packet is routed. To prevent other packets from traversing through the same region, local-maximum streets are marked as *OFF*. This route information is disseminated in the network, so as for these routes not to be used for anchor discovery. The protocol is simulated extensively in [10], compared to GSR and GPSR. It shows obvious network performance improvement.

P2P: A peer-to-peer approach for the support of traffic safety applications is presented in [8]. The vehicles (and potential road side access points[2]) communicate via an ad hoc peer-to-peer mechanism. The exchanged data is assumed to be describing vehicular motion, road properties and warnings or infotainment data, to facilitate traffic safety. However, the scheme can also be applicable for other types of applications. Moreover, even though

[2]The proposed architecture does not require any kind of infrastructure associated with roads.

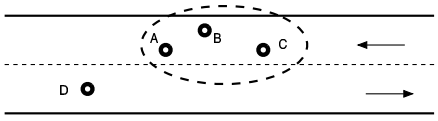

Fig. 1. Cluster-based organization

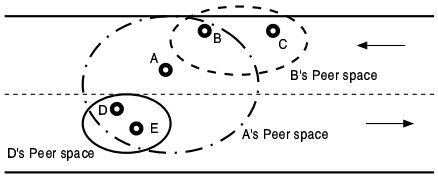

Fig. 2. Peer-centered organization

the paper assumes the existence of roadside servers or relays, all the network equipment is considered as part of the same vehicular network. Network nodes are called vehicular peers and they utilize ad hoc connectivity. They are organized in zones, called peer spaces, according to their common interests. Each peer in a peer space maintains information about all the other peers within the same peer space. Because the authors focus explicitly on traffic safety, they organize the peer spaces based on three issues: the communication region, the peer space composition and specific parameters of the driving situation. They argue that there is no advantage for a peer to maintain knowledge for many others. Thus each peer space includes at most a number of nodes; they set this to 15 peers. By this way information overflow and high overhead are avoided. Peer space organization can be either cluster-based or peer-centered.

Vehicles decide that their safety will benefit from associating with neighbors and thus form the peer spaces. An example is depicted in figure 1. Vehicle A exchanges information with vehicles B and C and realizes that this data is valuable; hence is joins their network. In contrast, node D considers this data useless, so it stays out of the peer space comprised by A, B and C. When a node leaves the cluster, all remaining nodes delete all data for it. Also if a peer does not receive information about clusters in the area, it will initiate its own peer space.

In the peer-centered organization each vehicle creates its own peer space. It analyzes data from other participants and decides which neighbor should be included in its dynamic peer space. Different peer spaces can be overlapped, as shown in figure 2.

The major difference between the approaches is that the peer-center assumes a peer as the core of a group. The network is organized according to individual preferences. As a result, such an approach is more appropriate for urban areas. In contrast, cluster-based is preferable for highway environments.

The architecture incorporates two kinds of routing: inter-space (between the peer spaces) and intra-space (within a peer space). Inter-space routing is associated with traffic safety, from the perspective of accident notification to many vehicles on the road. For intra-space routing the authors propose mediation mechanisms. All peers include in their packets the identities of the other peers that are known by senders to be registered in the same peer space. This information is stored by nodes that receive it. Highly inefficient flooding can be thus avoided.

The mediation mechanisms employed, differ for the cluster-based and peer-center approaches. For the former, they can be automatic or on demand. In automatic mediation, any peer analyses data that has for other peers. It can thus determine when a peer has no data for another peer in the space. In such a case it will retransmit the missing data. In the on-demand case, peers that are missing data for others, transmit certain messages requesting the missing data. For the peer-centered, mediation can be automatic only.

Other schemes: So far we discussed in some detail the most relevant related studies on vehicular network routing. Here we mention some additional work.

In [15] Saha and Johnson present a realistic model for vehicular motion, which they integrate in the famous *ns-2* simulator, and argue that their model is more accurate than the Random Way-point Model in some cases of vehicular movement. The region map is represented as a graph, in which vertices are the road intersections and edges are the road segments. Each node starts at a random point and moves towards another random point located on a random destination node. Dijkstra's algorithm is used to calculate the route and movement of the vehicle is constrained along this path.

Chisalita and Shahmehri in [9] propose a distributed protocol for decentralized network organization. The protocol requires the receivers to analyze the exchanged messages so as to figure out if they are the intended destinations. For this filtering the current traffic conditions are taken into account. The protocol includes mechanisms for message acceptance/denial, local maintenance of neighborhood information and transmission of basic safety (as well as non-safety) messages.

In [12] Agarwal et al. study the feasibility of mobile gateways in vehicular ad hoc networks, through simulations. They use a simple mobility model, and various aspects of connectivity along with routing performance are

evaluated. Simulation suggests that each vehicle should be able to connect to at least one gateway most of the time. The authors evaluate the effectiveness of the AODV routing protocol and conclude that it performs well, however they observe frequent link failures. To resolve this, they propose two simple prediction-based routing protocols to reduce those failures.

The discovery of Internet gateways by vehicles is investigated in [14]. Stationary Internet gateways are assumed at the roadside. Bechler et al. prove that current routing approaches and classic discovery protocols cannot address this requirement. They further propose *DRIVE*, a mechanism that efficiently discovers Internet Gateways. This service discovery protocol employs an automated method for selecting the most suitable gateway among the available ones. It uses a fuzzy-approach that considers the network properties and application classes. The location-based service discovery is also examined in [16]. Klimin et al. propose a mechanism based on geo-cast addressing of control messages. This hybrid approach combines request propagation reactively, with a proactive method for service advertisements. The advantage from this combination is twofold. First, clients are able to initiate discovery, even when they are located outside the proactive zone of a service provider. Second, intermediate nodes may reply to service requests on the border of the provider's proactive zone. This helps saving bandwidth and accelerates the discovery procedure.

V. Security Issues

A. *A quick revision*

Attacks cause anomalies to the network functionality. A lot of previous studies have investigated security vulnerabilities of routing protocols for wireless networks. These studies discuss the steps that certain attacks follow to harm the network. Such attacks can take advantage of algorithmic properties of the routing protocols. Also, there are attacks in which malicious nodes advertise fake locations to their neighbor nodes.

As for the first category, routing protocol designers need to incorporate security measures into the protocols. A designer needs to consider every aspect of his/her algorithm that could be utilized by malicious nodes. The network characteristics must also be taken into account. For example, situations in which the network topology changes dynamically, are tempting to attackers for various reasons. First of all, mobility allows a modification of the routing table of the victim node, simply by moving into the coverage range of it. The attacker may move away once it succeeds and without being traced. Moreover, the mobility of legitimate nodes may help attackers disperse their malicious information (epidemic spreading). Furthermore, the set of devices within the transmission range of a node keeps changing dynamically. Besides the algorithmic vulnerabilities, malicious attackers may damage the network, by announcing fake node locations. Such attacks are even more difficult to mitigate.

B. *The case of Vehicular Networks*

The unique properties of vehicular networks that we discussed earlier have an impact on attack effectiveness. First of all, attacks that target in exhausting the node battery are not applicable here. Vehicles have the ability of constantly charging their batteries. Moreover, the vehicle's power supply is more than enough to support energy-demanding computational systems. As a result, authentication processes do not have to be *light-weight*.

However, vehicular networks could suffer from other types of attacks. Specifically, in [5] Dousse et al. prove that the probability of end-to-end connectivity decreases with distance, for one-dimensional network topologies. This implies that it now becomes much easier for a malicious attacker to partition the network. This effect can potentially be addressed by maintaining multiple forwarding nodes for each packet. For example, in *MDDV* the protocol allows a group of vehicles near the *message head* to actively propagate the message. Hence, if we only have one or a few malicious nodes, the rest of them could potentially maintain the node reliability. However, a synchronized attack by multiple compromised vehicles would be disastrous. More than that, vehicular networks are expected to show large scalability. This, together with the unreliability of single vehicles, is ideal for applying even simple attacks.

On the other hand, even though vehicular movement can be quite fast, it is rather predictable. This does not mean that we can always know the exact direction of a vehicle; however, a probabilistic or stochastic approximation could be incorporated in previous authentication studies. Especially for location verification methods, the predicted mobility of the *claimant* could be easily employed from the verification algorithm. As a result, location estimation methods designed for traditional wireless networks can be adopted for vehicular networks, with minor modifications. No modifications may be required for some of them. This is because those mechanisms rely on signals transmitted either with the speed of light or with the speed of sound, or a combination of them. It is rather impossible that the average vehicle speeds will reach the speed of sound, at least in the near future, even

for highway environments. Hence the relative (to the mechanisms) vehicular speeds are not expected to affect the validity of these mechanisms. Our prediction could be supported by [6]; Wu et al. argue that the traffic in the opposite direction of the desired information flow is less helpful than the traffic in the same direction. Since the relative speeds in the same direction can be considered negligible, they will not affect the verification methods. This is because verifiers and claimant are expected to have the same approximate speed. In case the claimant travels in the opposite direction, it is less likely that it will be part of a network in its opposite direction. If this is the case however, it can be more difficult for verifiers to correctly estimate its actual location.

In [19] Zarki et al. discuss some general security and privacy issues. They present *DAHNI*, a simple vehicular communication infrastructure, without deeply analyzing its details. The article assumes no confidentiality for the transmitted data and that data is highly delay-sensitive. It is argued that:

1) No key distribution is usually required. No bulk data is transmitted and vehicles are not likely to stay in a cell for a long time.
2) Explicit handoffs are not required if communication is largely one-way (i.e. vehicles reporting their properties to the base station).

A potential simple security architecture for vehicular networks should at least include *(1)* Digital signatures, *(2)* Time-stamping and sequencing and *(3)* a certification infrastructure. Even though the authors do not proceed to some kind of implementation/simulation, their scheme seems resonable, while the required technology components are available nowadays.

VI. Conclusion

In this paper we investigated routing aspects of vehicular networks. We identified the potential wireless technologies, properties, architectures, security concerns and previous studies. After presenting proposed models, we commented on their efficiency and feasibility.

Vehicular networks are expected to be very attractive in the near future, facilitating numerous applications. However, to fully exploit their advantages, network designers need to take into account the unique characteristics of such networks.

References

[1] Q. Xu, R. Sengupta, and D. Jiang: "Design and Analysis of Highway Safety Communication protocol in 5.9 GHz Dedicated Short Range Communication Spectrum", IEEE VTC'03.

[2] L. Wischhof, A. Ebner, H. Rohling, M. Lott, and R. Hafmann: "Adaptive Broadcast for Travel and Traffic Information Distribution Based on Inter-Vehicle Communication", IEEE IV'2003.

[3] M. Bechler, W. Franz, and L. Wolf: "Mobile Internet Access in FleetNet", KiVS 2003.

[4] C. Lochert et al.: "A Routing Strategy for Vehicular Ad Hoc Networks in City Environments", Intelligent Vehicles Symposium, IV 2003, Ohio, USA.

[5] O. Dousse, P. Thiran, and M. Hasler: "Connectivity in ad-hoc and hybrid networks", IEEE INFOCOM 2002.

[6] H. Wu, R. Fujimoto, R. Guensler and M. Hunter: "MDDV: A Mobility-Centric Data Dissemination Algorithm for Vehicular Networks", 1st ACM Workshop on Vehicular Ad Hoc Networks, 2004.

[7] D. L. Gerlough and M. J. Huber: "Traffic flow theory: a monograph", Washington: Transportation Research Board, National Research Council, 1975.

[8] I. Chisalita, N. Shahmehri: "A Peer-to-Peer Approach to Vehicular Communication for the Support of Traffic Safety Applications", 5th IEEE Conference on Intelligent Transportation Systems, Singapure, Sept. 3-6, 2002.

[9] I. Chisalita, N. Shahmehri: "A context based vehicular communication protocol ", 2004 IEEE Personal, Indoor and Mobile Radio Communication Symposium, Barcelona, Spain 5-8 Sept. 2004.

[10] B. S. Lee, B. C. Seet, G. P. Liu, C. H. Foh, K. J. Wong: "A Routing Strategy for Metropolis Vehicular Communications", Proceedings of The International Conference on Information Networking (ICOIN'04), vol. 2, pp 533-542, Korea, Feburary 2004.

[11] H. Fssler, M. Mauve, H. Hartenstein, M. Ksemann, and D. Vollmer: "A comparison of routing strategies for vehicular ad-hoc networks", (poster), ACM MobiCom 2002.

[12] V. Namboodiri, M. Agarwal and L. Gao: "A study on the feasibility of mobile gateways for vehicular ad-hoc networks", Proceedings of the first ACM workshop on Vehicular ad hoc networks, pp. 66-75, 2004.

[13] J. F. Dillenburg, P. C. Nelson, and O. Wolfson: "Applications of a Transportation Information Architecture", IEEE ICNCS 2004.

[14] M. Bechler, O. Storz, W. Franz and L. Wolf: "Efficient Discovery of Internet Gateways in Future Vehicular Communication Systems", Proceedings of the 57th IEEE Semiannual Vehicular Technology Conference (VTC 2003 Spring), Jeju, Korea, April 2003.

[15] A. K. Saha, D. Johnson: "Modeling Mobility for Vehicular Ad Hoc Networks", Extended Abstract, Proceedings of the first ACM Workshop on Vehicular Ad Hoc Networks, pp.91-92, 2004.

[16] N. Klimin, W. Enkelmann, H. Karl and A. Wolisz: "Hybrid Approach for Location-based Service Discovery in Vehicular Ad Hoc Networks", WIT 2004: 1st International Workshop on Intelligent Transportation, 2004.

[17] D. Ghosal, C. N. Chuah, and M. Zhang: "VGrid/VMesh: Distributed Sensing and Computing with Vehicular Ad Hoc Networks", Technical Report ECE-CE-2004-9, Computer Engineering Research Laboratory, University of California, Davis, December 2004.

[18] M. Kasemann et al.: "A Reactive Location Service for Mobile Ad Hoc Networks", Technical Report TR-02-014, Department of Computer Science, University of Mannheim, 2002.

[19] M. El Zarki, S. Mehrotra, G. Tsudik and N. Venkatasubramanian: "Security Issues in a Future Vehicular Network", EuroWireless 2002, February 2002.