Information Dissemination and Information Assurance in Vehicular Networks: A Survey

Prashant Krishnamurthy

School of Information Sciences, University of Pittsburgh
135, N. Bellefield Avenue
Pittsburgh, PA 15260
+1 412-624-5144

prashant@sis.pitt.edu

ABSTRACT

Vehicular networks aimed toward providing roadside services such as traffic alerts, estimated time to reach a destination, alternative routes, and in general improve the efficiency and safety on the road are emerging in both the United States and Europe. Information exchange in such networks occurs between vehicles (inter-vehicle communications) in an ad hoc manner and also with roadside base stations using so-called dedicated short range communication links. Research on technology related to vehicular networks is being conducted by many universities and is being widely reported in the mainstream media as well. Vehicular networks are thus expected to become an important part of community networks of the future. In this paper we will survey the different types of dissemination of information and the assurance of such information in vehicular networks. The paper will discuss the architecture of vehicular networks, classify different types of information exchange (safety, traffic related, and content) and different methods of information exchange (opportunistic exchange of resources between vehicles, vehicle assisted data delivery, cooperative downloading of information, etc.). Then we discuss information assurance issues in vehicular networks and survey the solutions proposed for ensuring authenticity/integrity of information, location privacy of vehicles, eviction of faulty or misbehaving vehicles from the information network (e.g., using reputation), etc.

Topics

Community technologies and networking
Information assurance and security

Keywords

Vehicular networks, data aggregation, security, authentication

1. INTRODUCTION

Over the last four years, interest in vehicular networks has become resurgent. This is primarily due to the allocation of 75 MHz of *licensed* spectrum by the Federal Communications Commission in the 5.850-5.925 GHz range [1] for so-called *dedicated short range communications* (DSRC) for intelligent transportation system applications. This spectrum opened up new opportunities for realizing a variety of communications between vehicles – both vehicle-to-vehicle communications (V2V) and vehicle to roadside infrastructure (V2I) beyond what the previously allocated *unlicensed spectrum* in the 915 MHz range could offer. Such vehicular networks, aimed toward providing roadside services such as traffic alerts, estimated time to reach a destination, alternative routes, and in general improve the efficiency and safety on the road, are emerging in both the United States and Europe. The large bandwidth that is available also makes it feasible to envisage other applications such as downloading and sharing content between vehicles. The Association of Computing Machinery has organized four annual workshops on vehicular ad hoc networks (VANETs) since 2004. A special issue of the IEEE Journal on Selected Areas in Communications has been dedicated to this subject area [2], and several other conferences and venues have seen increased research activity related to ad hoc networks. Not only is research on technology related to vehicular networks being conducted by many universities, but it is being widely reported in the mainstream media as well [3]. Vehicular networks are thus expected to become an important part of community networks of the future.

In this paper we will survey the different types of dissemination of information and the assurance of such information in vehicular networks. The paper will discuss the architecture of vehicular networks, classify different types of information exchange (safety, traffic related, and content) and different methods of information exchange (opportunistic exchange of resources between vehicles, vehicle assisted data delivery, cooperative downloading of information, etc.). Then we discuss information assurance issues in vehicular networks and survey the solutions proposed for ensuring authenticity/integrity of information, location privacy of vehicles, eviction of faulty or misbehaving vehicles from the information network, etc.

The paper is organized as follows. In Section 2, we provide some background on the architecture of vehicular networks, the different standards bodies and consortiums working on vehicular networks, and other related material. Section 3 considers information dissemination in vehicular networks, the different types of information that is expected to be disseminated, the propagation of such information in the network, and methods to disseminate and acquire content. Section 4 looks at information assurance issues in vehicular networks and surveys the issues and techniques that have been discussed in the research literature. Finally, Section 5 provides some discussion of open topics and concludes the paper.

2. BACKGROUND

In this section, we present some background on the architecture of vehicular networks. It is assumed in much of the literature that position information is locally available to each vehicle with an error that is smaller than that needed for safety applications.

2.1 Network Architecture

In vehicular networks, it is expected that there will be limited access to an infrastructure network that will be supported by roadside base stations. Such access is limited in its nature for two reasons. First, the deployment of the infrastructure is expected to be slow and incremental leading to wide areas where there is no access to the infrastructure. Second, a complete deployment is expected to be sparse because of cost. The coverage provide by a roadside base station may be on the order of 200-300m while roadside base stations may be placed every km or so. Consequently, not all vehicles will be connected to the infrastructure at all times. To obtain access to safety or other types of information, it becomes necessary to rely on vehicle-to-vehicle communications.

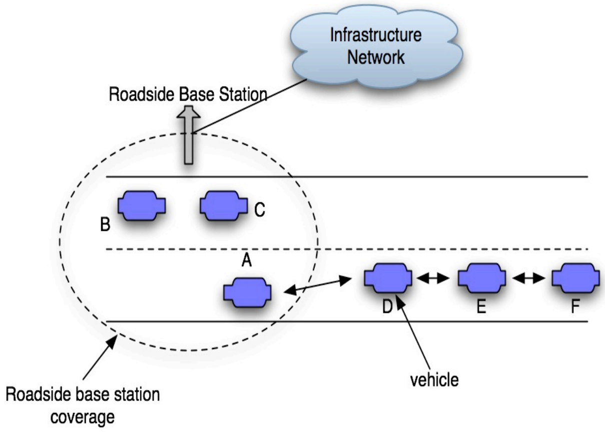

Figure 1: Schematic of a vehicular network architecture

As shown in Figure 1, vehicles A, B, and C have access to a roadside infrastructure, which has limited coverage. These vehicles can obtain information from the roadside base station. However, vehicles D, E, and F have no communications with the fixed infrastructure. For instance, Vehicle F will have to rely upon information from vehicle E, which in turn has obtained information that has passed through vehicles A and D.

Note that this scenario immediately creates issues that are not necessarily important in other kinds of networks in terms of how to disseminate information and how to assure the security of information. Note also, that vehicles that are in the range of a roadside infrastructure may be connected to the infrastructure for extremely small durations of time because of small coverage and high vehicular speeds. So the amount of information that can be pulled from the infrastructure is necessarily limited. It is also possible that vehicles move into the range of the roadside infrastructure with some information obtained from cooperating vehicles they have encountered. The issue then becomes one of updating the information, enhancing the reliability or relevance of information, or obtaining information that complements that already available to the vehicle.

2.2 Organizations and Standards

A variety of standards organizations and consortiums are actively involved in developing and promoting the technology for vehicular networks.

The IEEE is involved in standards related to the physical, medium access and security issues as well as in defining higher layer services and interfaces for intelligent transportation. By the end of 2006, the IEEE P1609 standards for wireless access in vehicular environments (WAVE) had specified the application layer and message formats for operation in the 5.9 GHz DSRC communications. The IEEE 802.11p standard [4], which is a modification of the popular IEEE 802.11 (Wi-Fi) standard, looks at issues related to the highly dynamic environment and the extremely short time durations where communications must be completed due to the high speed of the communicating vehicles.

Several consortiums with industry and/or public participation are also working on furthering the development and deployment of vehicular networks. Some examples are mentioned here. The Car-2-Car Consortium [5] comprising of automobile manufacturers, some universities and the Fraunhofer institute has as one of its primary objectives, the creation and establishment of an open and interoperable standard for V2V communications in Europe using Wi-Fi like components. Some communication protocols are being developed by the Network-on-Wheels (NOW) group, which is associated with the Car-2-Car Consortium [6]. Ford and General Motors created a Crash Avoidance Metrics Partnership (CAMP) and with the National Highway Transportation Safety Administration, this partnership is working on projects such as enhanced digital maps for safety, driver workload metrics and forward crash warning requirements [19].

3. INFORMATION DISSEMINATION

Information dissemination using DSRC is quite attractive due to the large bandwidth and the possibility of using multiple channels. The IEEE standards propose employing multiple 10 MHz channels, each capable of carrying 27 Mbps of data for vehicular communications. Up to seven channels are available in the 5.9 GHz bands and one channel is supposed to be dedicated for safety applications [7]. The remaining channels could potentially be used for content distribution and delivery. In this section, we describe the different types of information that need to be disseminated in a vehicular network and the methodologies that have been considered in the research literature.

3.1 Types of Information

It is expected that the large bandwidth of DSRC will enable a variety of yet to be anticipated applications for vehicular networks such as Internet extension, office on wheels, P2P file sharing etc.

[11]. The different types of information that need to be communicated and shared in a vehicular network can be classified into four categories: (a) safety information (b) traffic information (c) infotainment and other service information and (d) content. As discussed previously, information may be obtained partly from the roadside infrastructure and partly from other vehicles that are encountered by a given vehicle. In the case of many of the above types of information, the importance and relevance of the information changes with space and time [13]. For example, congestion information that is very far away may become increasingly important and need a more recent update as a vehicle gets closer to a congested area along with updates on alternative paths that may themselves have increased congestion by that point of time.

3.1.1 Safety Information

Safety information is the most important of the information types that are communicated in a vehicular network [8]. In 2006 alone, more than 42,000 people were killed in motor vehicle crashes in the United States [9]. In fact the primary purpose of DSRC is to greatly improve the safety of vehicular traffic. For example, DSRC can be used to prevent collisions between vehicles by providing information to the driver about whether the vehicle ahead is braking, if the speed is too high or the distance to other vehicles or objects is getting too close. Eight safety applications based on deliberations between government agencies and private industry have been identified in [10], which are traffic signal violation warnings, curve speed warnings, emergency electronic brake lights, pre-crash warnings, cooperative forward collision warnings, left-turn assistance, lane change warning and stop-sign movement assistance. Each of these applications makes use of high level data elements such as acceleration (in various quantization levels), obstacle direction, wheel angle, vehicle width etc. (see [10] for more details). Latency associated with many of these safety messages is crucial. The time taken by the driver of a motor vehicle to react to warnings has to be considered while delivering information to him/her [8], introducing the human component into the picture. The density and environment in which a vehicle is operating also influence the delivery of safety messages.

3.1.2 Traffic Information

This class of information primarily accounts for congestion on current roads, suggestions for alternative paths to the destination, road construction information etc. that are useful for safety and efficiency, but less time-critical than the “life safety” messages discussed earlier. However, traffic information may still have a higher priority than infotainment or content.

3.1.3 Infotainment and Services

DSRC can also be the mechanism for obtaining infotainment and location based services (e.g., where is the nearest coffee shop, or buying a ticket to a movie en route to the theater), using digital cash for paying tolls, and so on. This could also include information such as available parking spaces in the vicinity [13].

3.1.4 Content

Recent research work in vehicular networks have focused on content distribution [11, 12, 13, 14, and 15]. What differentiates content from infotainment and services is the quantity o information. In most of the research literature cited above, the assumption is that vehicles will be interested in obtaining extremely large files (e.g., video on demand) that cannot be obtained through a few limited transactions with either the roadside infrastructure or a couple of nearby vehicles. The efficient *discovery* and *distribution* of large quantities of information is a challenging problem especially in a dynamic environment.

3.2 Information Dissemination Methods

Dissemination of the various types of information poses numerous challenges in vehicular networks because of many reasons. The size of the network, the speed of vehicles, the patchy and intermittent connectivity with both the roadside base stations where they exist and between vehicles as they move, the significance and germaneness of the information that changes with vehicular position and time are only a few of these reasons. Safety information has critical latency requirements [8]. Content needs to be efficiently discovered and shared. In what follows, we look at the attempts in the research literature to address several open problems that remain with respect to information dissemination in vehicular networks.

In order to evaluate the methods for disseminating information, models that capture the idiosyncrasies of vehicular networks are necessary. However, such models are not widely available. In [7], a large scale simulator of vehicular networks has been developed and utilized for freeway scenarios. Simulation models for urban settings that include street layout, traffic rules (like stop signs), multi-lane roads, the slowing down and speeding up of vehicles, and attenuation of communication signals with distance are captured in [20]. The importance of such models cannot be emphasized. Efficient and reliable dissemination of information will be impacted by how vehicles are clustered, when they form and leave groups, how far apart they are under different traffic conditions, the density of vehicles etc. Realistic vehicular traces were used with simulations in [21] and the authors demonstrated that such real traces show noticeable differences compared to widely used mobility models. For instance, vehicles merge into groups ahead of them when they are faster and break away (or split) from groups if they are slower. For example, if al vehicles are moving to the right in Figure 1, vehicle F could eventually split from vehicles D and E if it moves faster. Handling such mergers and splits can impact packet delivery [21] and thus information dissemination. In [16], the spatial propagation of information is analytically investigated and shown to depend on vehicle density, speed etc.

Methods of delivering information vary in the research literature. Information may be *opportunistically* pulled from other vehicles or the infrastructure as a target vehicle encounters them [13]. In an different scenario, a vehicle carries information with it and delivers it either to the infrastructure or to other vehicles when it encounters them, using mobility in addition to wireless transmissions to disseminate information [17]. This process is called *vehicle-assisted delivery*. For content delivery, vehicles can download partial units of some content and share them afterwards to obtain the complete content. This has been called *cooperative downloading* [12].

In the case of safety information (and certain types of traffic and service information – e.g., availability of parking space), the temporal and spatial delivery of information have to be carefully considered. For instance, it becomes necessary to evaluate how far the information should be disseminated [8] and this depends on the traffic conditions (e.g., information need be propagated over shorter distances in the case of a traffic jam). In [7], simulations of forward collision warning in a freeway scenario were conducted. Under the assumption that every vehicle periodically reports its information, the density of vehicles and their distance from the target vehicle determined the success of delivery of packets at the target vehicle. One suggestion by the authors there is to thus reduce the transmission range of vehicles to improve packet success probability.

In the case of traffic and service information, aging of the information with time and distance is suggested in [13]. Information is opportunistically pulled from neighboring vehicles as a target vehicle moves in a given area. Such information needs to have a time stamp and a location stamp. As the vehicle moves farther away from where the information is relevant or as time elapses, the information is aged and eventually purged. This enables vehicles to maintain up-to-date information without taxing memory and other resources. The propagation and survival of information is discussed in [13] and [16], both in time and space. Because of the spatio-temporal relevance of information, a piece of information tended not to propagate beyond a specific boundary. In time, a given piece of information would propagate very quickly till it reaches a maximum number of copies and then it would also rapidly decline from that point.

Recent papers have addressed content distribution in vehicular networks. The primary idea here is that vehicles download pieces of files when they have access to the roadside and then share such pieces with one another. Eventually they all have the required file. The sporadic nature of connectivity makes this problem difficult. In [12] and [14], content is partially downloaded from a roadside base station, which also provides a list of other vehicles that have parts of the file. Each vehicle then "gossips" about what part of the content it has. Preference is given to local neighbors to download remaining parts of the file. A closest-rarest strategy is adopted where the rarest piece of the file is downloaded first. This approach resembles BitTorrent [12], but is decentralized and employs proximity information to improve performance. This is because multihop communications degrade the performance of information delivery rapidly as the number of hops increase. In [11], network coding and mobility assistance (as in [17]) along with gossiping (as in [12]) is employed with *only single hop* distribution of content to further improve performance. A single hop content distribution is also proposed in [15]. Broadcasting replicas of pieces of files at the intersections of roads so as to reach a large number of vehicles is suggested in [22].

3.3 Data Aggregation

As previously mentioned, flooding the network with information reduces the performance in terms of latency, packet loss, and reliability. Also, the relevance of information decreases with space and time. Recently, data aggregation schemes have been proposed to reduce the load on the network, yet make useful information available to vehicles that may be far away. In [23], vehicles first produce a *primary data record* that is made up of the vehicle's location, speed, time stamp, etc. Clusters of vehicles create a *local view* and local views are periodically aggregated into *cluster records*. Aggregate information is disseminated in the network. In [24], the difficulty of *comparing* aggregate information in vehicular networks is discussed. The problem here is how a vehicle should decide which aggregate is *better* to use, since different aggregates may have included different individual changed observations. This problem is addressed by using an approximate representation of data in the form of a modified Flajolet-Martin sketch, that enables aggregation of two aggregated data sets, thereby eliminating the problem of comparison.

4. INFORMATION ASSURANCE

Assuring information in vehicular networks has unique challenges due to some of the same reasons as information dissemination, namely the size of the network, the speed, the dynamic topology, the intermittent connectivity, lack of trust between vehicles, etc. The differing requirements of the different types of information in vehicular networks further complicate information assurance (e.g., latency is an important issue for "life-safety" information while it is not crucial for content delivery). Only recently has some attention been placed on the security of vehicular networks. A discussion of the vulnerabilities and challenges for securing vehicular communications is presented in [18].

Considering the usual information assurance services, i.e., confidentiality/privacy, authentication, integrity, availability and non-repudiation, it is easy to see how vehicular networks are vulnerable. Since the location information of vehicles is disseminated, there is a serious question of location privacy. Authenticating messages and ensuring their integrity become very important to make certain that fabricated messages do not cause dangers to safety in the worst case or cause traffic jams in the best case. A vehicle must not deny being the cause of an accident if it indeed was responsible for it, nor should the blame be placed on another vehicle. Simple techniques like jamming of signals can severely impact the safety of the vehicular network by affecting the availability of information. Distribution of content in vehicular networks raises its information assurance challenges that have hardly been considered in the research literature.

In [18] a security architecture is presented that provides information assurance using tamperproof security hardware and a vehicular public-key infrastructure to provide information assurance. Privacy is enabled using anonymous keys, pre-loaded into the tamper-proof hardware, but which can be tracked back to an electronic license plate if law enforcement needs it. In [26], the use of multiple credentials to decouple the identity of the vehicle from its keys to potential eavesdroppers is proposed. This scheme thus maintains privacy of the vehicle. Public key algorithms and protocols are however bandwidth intensive (making use of certificates) and may adversely affect latency requirements of safety information. Symmetric encryption creates its own set of problems because of the necessity of a trusted roadside infrastructure to distribute and manage keys. To solve this problem, an identity based security framework for vehicular networks is proposed in [25]. This makes use of Weil-Tate pairings where arbitrary strings can act as public keys that can maintain privacy while reducing the number of communicated messages.

Despite all precautions, it is possible that malicious nodes will send fabricated information to disrupt the operation of vehicular networks. In [27], data validation is used to detect such fabricated information under the assumption that honest vehicles are more prevalent than malicious ones. Sybil attacks, where a malicious node can claim to have several identities each bolstering its fabricated claim, are thwarted by distinguishing vehicles (two vehicles cannot occupy the same position at the same time). Position information is similarly exploited to prevent Sybil attacks in [28]. [29] also discusses approaches to prevent vehicles from fabricating their position information.

Data aggregation is quite important for maintaining the performance of vehicular networks and ensuring information dissemination. References [30] and [31] consider secure data aggregation for vehicular networks.

Finally, detection, isolation, and eviction of malicious or faulty vehicles from a vehicular network is discussed in [32].

5. DISCUSSION AND CONCLUSIONS

Vehicular networks, as they are conceptualized today, are already quite complex. However, the applications, and usage scenarios are unpredictable till such networks are actually deployed, and widely utilized. For example, the burgeoning of community Wi-Fi networks was never anticipated in the early days of its inception. It is quite possible that user communities of vehicular networks may arise (as against autonomous vehicular communities or clusters) and people will choose to use such networks in ways that are unique and challenging in terms of information dissemination and assurance. Already, content distribution could be a problem. There are no good mechanisms for ensuring rights management in an environment with good connectivity, let alone in one with limited or intermittent connectivity. The evolution of vehicular networks will also depend on how "open" they are. The safety requirements will make it necessary to close at least some parts of the network to ensure limited or no disruption to vehicular safety.

In this paper, a survey of recent research in the areas of information dissemination and assurance in vehicular networks was presented. The paper discussed the architecture of vehicular networks, classified different types of information exchange (safety, traffic related, and content) and different methods of information exchange. Then we discussed information assurance issues in vehicular networks and surveyed the solutions proposed for ensuring authenticity/integrity of information, location privacy of vehicles, eviction of faulty or misbehaving vehicles from the information network.

6. REFERENCES

[1] See http://www.fcc.gov/services for a list of wireless services and DSRC is listed therein. The link to DSRC provides additional information.

[2] IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks, October 2007.

[3] Roy Furchgott, "Navigating With Feedback From Fellow Drivers," New York Times, October 18, 2007.

[4] The IEEE 802.11Task Group p to define enhancements to 802.11 required to support Intelligent Transportation Systems available at: http://grouper.ieee.org/groups/802/11/Reports/tgp_update.htm

[5] Car-2-Car Communication Consortium at: http://www.car-2-car.org

[6] Network-OnWheels at: http://www.network-on-wheels.de/

[7] T. ElBatt *et al.*, "Cooperative Collision Warning Using Dedicated Short Range Wireless Communications," *Proc. ACM Workshop on Vehicular Ad Hoc Networks (VANET)*, September 2006.

[8] Q. Xu, T. Mak, and R. Sengupta, "Vehicle-to-Vehicle Safety Messaging in DSRC," *Proc. ACM Workshop on Vehicular Ad Hoc Networks (VANET)*, October 2004.

[9] "Traffic Safety Facts," 2006 Overview Data available at the National Highway Transportation Safety Aministration's website at http://www.nhtsa.gov.

[10] C. L. Robinson, *et al,* "Efficient Coordination and Transmission of Data for Cooperative Vehicular Safety Applications," *Proc. ACM Workshop on Vehicular Ad Hoc Networks (VANET)*, September 2006.

[11] U. Lee *et al.*, "CodeTorrent: Content Distribution Using Network Coding in VANET," *Proc. ACM Mobishare*, Los Angeles, September 2006.

[12] A. Nandan et al., "Co-operative downloading in vehicular ad-hoc wireless networks," *Second IEEE Conference on Wireless On-demand Network Systems and Services*, January 2005.

[13] B. Xu, A.Ouksel, O. Wolfson, "Opportunistic resource exchange in inter-vehicle ad-hoc networks," *Proc. IEEE Int. Conf. on Mobile Data Management*, pp. 4-12, 2004.

[14] S. Das *et al.*, "SPAWN: A Swarming Protocol for Vehicular Ad Hoc Wireless Networks," *Proc. ACM Workshop on Vehicular Ad Hoc Networks (VANET)*, October 2004.

[15] M. Fiore, C. Casetti, C-F Chiasserini, "On-demand Content Delivery in Vehicular Wireless Networks," *Proc. MSWiM*, October 2005.

[16] H. Wu et al., "Analytical models for information propagation in vehicle-to-vehicle network," *Proc. IEEE Vehicular Technology Conference*, 2004.

[17] J. Zhao and G. Cao, "VADD: Vehicle-Assisted Data Delivery in Vehicular Ad Hoc Networks," *Proc. IEEE Infocom*, 2006.

[18] M. Raya, P. Papadimitratos, J-P. Hubaux, "Securing Vehicular Communications," *IEEE Wireless Communications*, October 2006.

[19] Crash Avoidance Metrics Partnership at: http://www.camp-ivi.com/

[20] A. Mahjan, N. Potnis, K. Gopalan, and A. Wang, "Modeling VANET Deployment in Urban Settings," *Proc. ACM MSWiM*, October 2007.

[21] V. Naumov, R. Baumann, T. Gross, "An Evaluation of Inter-Vehicle Ad Hoc Networks Based on Realistic Vehicular Traces," *Proc. ACM Mobihoc*, May 2006.

[22] M. Yamanaka, G. Tsuchida, S. Ishihara, "A Replica Distribution Scheme for Location Dependent Information in Vehicular Ad Hoc Networks," *Proc. ACM Workshop on Vehicular Ad Hoc Networks (VANET)*, October 2006.

[23] K. Ibrahim and M.C. Weigle, "Accurate Data Aggregation for VANETs," *Poster in Proc. ACM Workshop on Vehicular Ad Hoc Networks (VANET)*, September 2007.

[24] C. Lochert, B. Scheurmann, M. Mauve, "Probabilistic Aggregation for Data Dissemination in VANETs," *Proc. ACM Workshop on Vehicular Ad Hoc Networks (VANET)*, September 2007.

[25] P. Kamat, A. Baliga, and W. Trappe, "An Identity Based Security Framework for VANETs," *Proc. ACM Workshop on Vehicular Ad Hoc Networks (VANET)*, September 2006.

[26] G. Caladriello, P. Papadimitratos, J-P Hubaux, "Efficient and Robust Pseudonymous Authentication in VANET," *Proc. ACM Workshop on Vehicular Ad Hoc Networks (VANET)*, September 2007.

[27] P. Golle, D. Greene, and J. Staddon, "Detecting and Correcting Malicious Data in VANETs," *Proc. ACM Workshop on Vehicular Ad Hoc Networks (VANET)*, October 2004.

[28] G. Yan, G. Choudhary, M. Weigle, S. Olariu, "Providing VANET Security Through Active Position Detection," *Proc. ACM Workshop on Vehicular Ad Hoc Networks (VANET)*, September 2007.

[29] T. Leinmuller *et al,* "Improved Security in Geographic Ad Hoc Routing through Autonomous Position Verification," *Proc. ACM Workshop on Vehicular Ad Hoc Networks (VANET)*, September 2006.

[30] F. Picconi *et al*, "Probabilistic Validation of Aggregated Data in Vehicular Ad Hoc Networks," *Proc. ACM Workshop on Vehicular Ad Hoc Networks (VANET)*, September 2006.

[31] M. Raya, A. Aziz, and J-P Hubaux, "Efficient Secure Aggregation in VANETs," *Proc. ACM Workshop on Vehicular Ad Hoc Networks (VANET)*, September 2006.

[32] M. Raya, *et al*., "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," *IEEE Jornal on Selected Areas in Communications*, Vol. 25, No. 8, October 2007.