Leveraging Dedicated Short-Range Communication for Enhanced Vehicle-to-Infrastructure Safety

Annie Abraham*¹ & Prof. Sheeba Paul²

*1&2Mar Athanasius College of Engineering

ABSTRACT

Many wireless communication systems are available now, which facilitate a wide range of applications and benefits in the vehicular environment. These applications can be organize into two types, namely, lane safety and traffic efficiency where each have its own set of functional and performance requirements. For ancillary drivers to travel safely and comfortably, many of these requirements need to be met. Also the harmony of different radio access technologies brings limitless opportunities for showdown the application requirements, it is very important and assert to note the toughness and vulnerability of each technology and get an idea about which technology is more suitable for the given networking scenario. In ITS, we need to deal with both vehicles and the road side units which is very important to bring these systems to awareness. In this paper, Dedicated Short Rang communication technique is used for improved road safety with aid of Secure Prediction based authentication scheme. Here, Beacons are used for secure V2V and V2R communication. When a large number of beacons arrive in a short time, vehicles are vulnerable to computation-based Denial of Service (DoS) attacks that excessive signature verification exhausts their computational resources. In contrast to most existing authentication schemes, our SPBAis an efficient and lightweight scheme since it is primarily built on symmetric cryptography. To further reduce the verification delay for some emergency applications, SPBA is designed to exploit the sender vehicle's ability to predict future beacons in advance. In addition, to prevent memory-based DoS attacks, SPBA only stores shortened re-keyed Message Authentication Codes (MACs) of signatures without decreasing security

KEYWORDS: Dedicated Short Range Communication, ITS, Denial of Service (DoS), Computational based Dos

I. INTRODUCTION

Many believe that the integration of information and communication technologies with transportation infrastructure and vehicle will revolutionize the way we travel today. The enabling technologies envisioned to realize the proposed framework would spur an array of applications and use cases in the domain of road safety, traffic efficiency, and infotainment. These applications allow dissemination and gathering of useful information among vehicles and between transportation infrastructure and vehicles in pursuance of assisting drivers to travel safely and comfortably. Reliable and low-latency communication between vehicles and transport infrastructure is critical to the implementation success of many of these applications. Vehicular networking is the enabling technology which allows the realization of the variety of applications and use cases. By using a Dedicated Short-Range Communications (DSRC) [1] technique, vehicles equipped with wireless On-Board Units (OBUs) can communicate with other vehicles and fixed infrastructure, e.g., Road-Side Units (RSUs), located at critical points of the road [2].

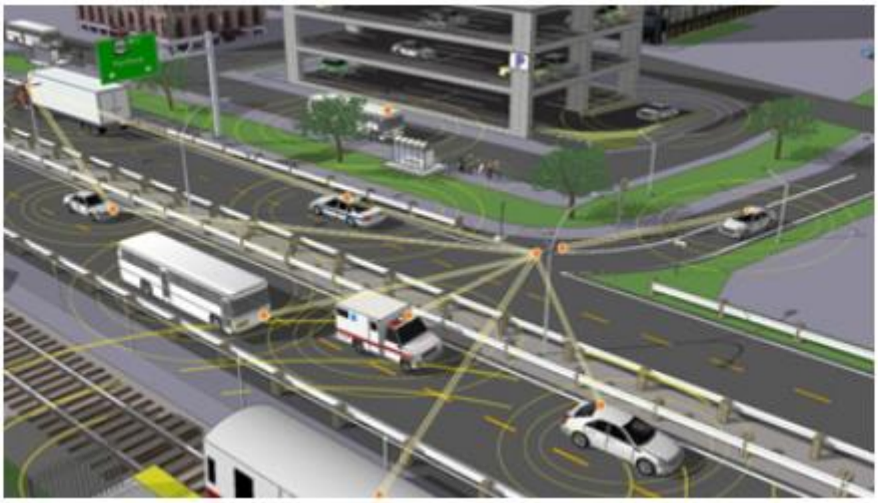

Figure1: VANET Scenario

Therefore, Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications are regarded as two basic types of communications in VANETs. Once VANETs become available, numerous safe, commercial and convenient services can be deployed through a variety of vehicular applications. These applications mostly rely on vehicles' OBUs to broadcast outgoing beacon messages and validate incoming ones. The broadcast beacons often contain information about position, current time, speed, direction, driving status, etc. For example, by frequently broadcasting and receiving beacons, drivers are better aware of obstacles and collision scenarios. They may act early to avoid any possible damage, or to assign a new route in case of a traffic accident in the existing route.

To secure vehicular networks, an authentication scheme is indispensable to ensure messages are sent by legitimate vehicles and not altered during transmissions. Otherwise, an attacker can easily disrupt the normal function of VANETs by injecting bogus messages. Therefore, vehicles should broadcast each message with a digital signature. However, the current VANET signature standard [6] using Elliptic Curve Digital Signature Algorithm (ECDSA) would cause high computational overhead on the standard OBU hardware, which has limited resources for cost constraints. Prior work has shown that one ECDSA signature verification requires 20 milliseconds on a typical OBU with a 400 MHz processor [7]. When a large number of signed messages are received in a short time period, an OBU cannot process them before their dedicated deadline. In this paper, we define this attack as computation-based Denial of Service (DoS) attacks. Even without any malice, the computation based DoS attacks can be easily initiated in a high density traffic scenario. For example, when traffic related messages (beacons) are sent 10 times per second as suggested by the DSRC protocol [1], [6], a vehicle is overwhelmed with more than five neighbors within its radio range. To defend against such attacks, most existing schemes [8], [9], [10] make use of the technology of identity-based batch verification [11] or aggregate signature [12] built on asymmetric cryptography to improve the efficiency of verification. In their schemes, the computational cost is mainly dominated by a few operations of pairing and a number of operations of point multiplication over the elliptic curve [13]. It is affordable for RSUs, but expensive for OBUs to verify the messages [14]. Furthermore, if attackers inject false beacons, the receiver is hard to locate them so that these schemes are also vulnerable to the computation-based DoS attacks [15]. Therefore, designing an effective authentication scheme under high-density traffic scenarios is a big challenge for V2V communications. In this paper, we propose an effective broadcast authentication scheme: Secured Prediction-based Authentication (SPBA) to defend against computation-based DoS attacks for V2V communications. Unlike most of existing schemes based on asymmetric cryptography [8],[9], [10], [15], [16], [17], [18], [19], [20], our SPBA is primarily implemented on symmetric cryptography, whose verification is more than 22 times faster than ECDSA. In addition, SPBA resists packet losses naturally. Similar to mobile wireless networks, packet losses are common in VANETs.

SPBA also aims at improving the efficiency of authentication. Certain vehicular applications may require receivers to verify urgent messages immediately. To support instant verification, we exploit the property of predictability of a future beacon, constructing a Merkle Hash Tree (MHT) [25] to generate a common public key or predication outcome for the beacon. With the prediction outcome known in advance, receivers can instantly verify the incoming beacon. Furthermore, we examine the storage overhead brought by our authentication scheme. If a mechanism brings a large storage burden, an attacker would initiate memory-based DoS attacks where an OBU is overwhelmed by storing a large number of unverified signatures. To defend against such attacks, SPBA records shortened re-keyed Message Authentication Codes (MACs) instead of storing all the received signatures.

II. WORKING OF VANET

VANET is a technology that uses moving vehicles as nodes in a network to create a mobile network. VANET turns every participating vehicle into a wireless router or node, allowing vehicles approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As vehicles fall out of the signal range and drop out of the network, other vehicles can join in, connecting vehicles to one another so that a mobile Internet is created. VANET is a subgroup of MANET where the nodes refer to vehicles. Since the movement of Vehicles are restricted by roads, traffic regulations we can deploy fixed infrastructure at critical locations. The primary goal of VANET is to provide road safety measures where information about vehicle's current speed, location coordinates are passed with or without the deployment of Infrastructure. Apart from safety measures, VANET also provides value added services like email, audio/video sharing etc,.Classes of Information:

- Movement Related –speed, velocity, acceleration, etc
- Traffic Related –number of vehicles, traffic volume, density, congestion
- Passenger Related –weather related information

In cryptography, a message authentication code (MAC) is a short piece of information used to authenticate a message in other words, to confirm that the message came from the stated sender (its authenticity) and has not been changed in transit (its integrity). VANETs are a subset of mobile ad hoc networks composed of network - equipped vehicles and infrastructure points, which will allow vehicles to communicate with other vehicles and with roadside infrastructure points. A Trusted Authority, which is responsible for providing anonymous certificates and distributing

Secret keys to all OBU in the network. So that communication overheads and consumes delay in message authentication. VANET can offer various services and benefits to users and thus deserves deployment effort. Attacking and misusing such network could cause destructive consequences. It is therefore necessary to integrate security requirements into the design of VANETs and defend VANET systems against misbehavior, in order to ensure correct and smooth operations of the network. A security system for VANETs to achieve privacy desired by vehicles and traceability required by law enforcement authorities, in addition to satisfying fundamental security requirements including authentication, nonrepudiation, message integrity, and confidentiality. The Road side unit plays a vital role in identifying the malicious node packets and clears those packets with correct packets with respect to all the vehicles in the scenario.

III. LITERATURE SURVEY

In this section, we present some of the most suitable multihop broadcast schemes proposed to deliver alert messages (e.g., in case of an accident), to advertise critical situations on the road, or those situations having similar requirements and that can equally benefit from this type of solution.

(i) The *counter-based scheme* proposed by Tseng et al. [5] was initially proposed for MANETs. More specifically, this scheme monitors the number of receptions of a broadcast packet by means of a counter c and a threshold C. If $c \geq C$ for a received message, rebroadcast is not allowed.

(ii) In the *distance-based scheme* [5], the rebroadcast of a message is determined by the distance d between sending and receiving vehicles. In particular, it is not recommended to rebroadcast it when vehicles are closer, since the *additional coverage* (AC) obtained by doing so is low and the maximum benefit of forwarding is achieved when the additional coverage is maximized [5].

(iii) The *slotted p-persistence* and the *weighted p persistence* schemes proposed by Wisitpongphan et al. [41] are broadcast storm mitigation techniques based on probabilities, where vehicles with a higher priority are allowed to use the channel in the least possible time. These techniques are among the few rebroadcast techniques conceived specifically for broadcast storm alleviation in VANETS, although their particular design makes them mostly suitable for highway scenarios since performance problems emerge in urban scenarios.

(iv) The Last One (TLO) is a scheme proposed by Suriyapaibonwattana and Pomavalai [42] where whenever a vehicle sends a warning message, there is a search process to locate the farthest reachable vehicle, which will be the only one granted to forward the packet. The distances between the sender and the rest of receiving vehicles are computed by means of positioning information gathered by GPS devices. This method is simple and enhances performance when compared to simple rebroadcasting, but since it does not account for urban obstacles like buildings in wireless communications, it is only effective in highway environments. In addition, it is unclear how vehicles are able to estimate the position of neighbor nodes when this information is needed.

(v) The *Adaptive Probability Alert Protocol* (APAL) is an extension to the TLO scheme including adaptive wait-windows and introducing different transmission probabilities [43]. This scheme outperforms TLO, but it still presents the same limitations regarding the situations where it is applicable, being only assessed in simple highways.

(vi) The stochastic broadcast scheme (SBS) was presented by Slavik and Mahgoub [44] with the goal of obtaining anonymity and scalability. In particular, nodes use a retransmission probability function to forward messages. The behavior of this scheme is affected by the vehicle density, and so this probability needs to be tuned for each specific scenario. Additionally, SBS was only tested in obstacle-free scenarios, and the influence of buildings on radio signal propagation has not been studied so far.

(vii) The *enhanced Street Broadcast Reduction* (eSBR) [45] uses the information obtained from the maps and the GPS to enhance alert message delivery in VANETs. One of the following conditions must be fulfilled for a vehicle to rebroadcast: (i) it must be located far away from the sender (>$d$min), or (ii) the receiving vehicle is located in a different street, thus accessing to other areas of the map. eSBR uses the roadmap data to overcome blind areas since buildings usually block the wireless signal, preventing the communication among vehicles.

(viii) Fogue et al. presented the *enhanced Message Dissemination for Roadmaps* (eMDR) [46], which is an extension to eSBR. The eMDR scheme attempts to reduce even more the amount of messages produced by avoiding to rebroadcast the same warning message multiple times. Information about the junctions present in the roadmap is used, so that only one of the vehicles located in each junction

is allowed to forward the warning message (specifically, the closest node to the center of the intersection in the map). Authors show that this mechanism is able to diminish the number of rebroadcasts required without reducing the rate of vehicles receiving warning messages.

(ix) The Connected Dominating Set (CDS) proposed by Ros et al. [47] employs periodic beacon messages to compute information about local positions in order to enhance the dissemination process. In particular, these beacons are used to determine whether the vehicles belong to a CDS in order to benefit from shorter retransmission waiting periods. Broadcast messages identifiers are included into the beacons as piggybacked acknowledgments. Therefore, after the expiration of the waiting timeout, the messages are retransmitted by vehicles in case that one of their neighbors did not acknowledge their correct reception.

(x) Sommer et al. presented the Adaptive Traffic Beacon (ATB) [48], a message dissemination protocol which is completely distributed and employs two key metrics to adapt beaconing: channel quality and message utility. Results showed that, compared to flooding based approaches, adaptive beaconing provides better dissemination, although at a slower rate. The goals of this scheme are twofold: sending beacons as often as possible so as to exchange information contained in knowledge bases and achieving a congestion-free wireless channel.

(xi) Bi et al. proposed the Cross Layer Broadcast Protocol (CLBP) [49], a dissemination scheme that selects appropriate forwarding vehicles considering (i) the channel conditions, (ii) the geographic positions, and (iii) speed of cars. Reliable transmissions in CLBP are achieved by sending *Broadcast Request To Send* and *Broadcast Clear To Send* messages. The CLBP has the goal of reducing the transmission delay, but it is only designed to work in single-direction and highway scenarios. In addition, it has not been tested in urban environments.

IV. EXISTING VANET-RELATED SURVEYS

Although some works (e.g., [9]) have surveyed existing broadcast protocols for mobile ad hoc networks (MANETs), to the best of our knowledge there are no specific VANET oriented works offering an overview of recent dissemination approaches In fact, despite the importance of warning message dissemination schemes in ITS safety applications, there is no survey so far that clearly presents and discusses the most relevant approaches proposed regarding warning message dissemination in VANETs. Additionally, existing proposals are usually evaluated under different conditions, making it quite difficult to determine what the best dissemination scheme for each specific scenario is. Below, we introduce some of the most relevant VANET-related surveys available. Cheng et al. [10] presented VANET data dissemination results by structuring surveyed techniques into three categories: unicast, multicast, and geocast/broadcast techniques, describing the most important ideas in each category. They also considered location services and security issues, in the context of data dissemination in VANETs. Unlike our work, authors did not provide any comparative analysis in terms of dissemination performance of the different approaches studied. Panichpapiboon and Pattara-Atikom [11] classified and provided an in-depth review of existing broadcasting protocols for VANETs. Despite the quality of this work, authors did not provide a thorough analysis of the characteristics of the protocols studied, nor was a fair comparison done. In particular, we consider carrying out an unbiased comparison essential that is, under the same simulation environment, thereby providing researchers clear guidelines to accurately assess their proposals. X. Li and H. Li [12] presented the most representative results of data dissemination in vehicle-to-vehicle (V2V) communications. In particular, their review was divided into three sections: routing protocols, mobility model, and security issues. Regarding VANET mobility models, Harri et al. [13] presented a procedure for the implementation of vehicular mobility models. In addition, they introduced the different existing approaches for vehicular mobility and their relationship with network simulators. They also proposed a taxonomy of some existing mobility models commonly used when simulating vehicular ad hoc networks. More recently, Jia et al. [14] presented a comprehensive study of platoon-based vehicular cyber-physical systems (VCPS).They also introduced two primary approaches based on VCPS, that is, the traffic dynamics, as well as the vehicular networking architecture and standards. Although several authors have published surveys focused on different issues related to vehicular networks such as mobility models [13, 15], security attacks [16], revocation [17], or routing [18–20], none of these works specifically focused on the warning message dissemination process, nor on the broadcast schemes used when dangerous situations take place. Moreover, existing works usually assess their proposals in very specific scenarios, with different vehicles densities, and under a wide variety of simulation tools. Therefore, unlike other surveys, in this work we assess the behavior of the most relevant existing broadcast dissemination protocols, evaluating them fairly, that is, under the same conditions, under same network model, and under same simulation tool and using the same performance metrics. We consider that such a fair evaluation is able to shed some light on the advantages and drawbacks of each solution, making it possible to determine which one is the most suitable scheme to be used on each particular scenario.

V. SYSTEM DESIGN

In this section, we present the proposed system design of Secure Prediction Based Authentication (SPBA).

Fast Auth Scheme

One-time signature scheme named Fast Auth is used to provide lightweight, timely and nonrepudiation authentication for vehicle-to-vehicle communications. Chained Huffman hash trees is use to generate a common public key and minimize the signature size for beacons sent during one prediction interval. Exploits the predictability of future beacons to achieve the instant authentication in VANETs.

- If the receiver misses a beacon, it cannot work in the rest of the current prediction interval.
- It cannot accurately collect the entire beacon message
- Also, it cannot increase the packet delivery ratio.

Secure Prediction Based Authentication System Module

The following are the details in the sender side and receiver side details involved in the communication.

Overview of Secure Prediction Based Authentication Scheme

Secure Prediction based authentication is used in the sender side to detect Denial-of-Service attacks before the signature verification. Enhanced attacked packet detection algorithm is used at the receiver side to detect malicious node. To reduce the verification delay, SPBA is designed to exploit the sender vehicles ability to predict future beacons in advance. Applications rely on vehicles OBUs to broadcast outgoing beacon messages and to validate incoming ones. The broadcast beacons often contain information about position, current time, speed, direction, driving status, etc. By frequently broadcasting and receiving beacons, drivers are better aware of obstacles and collision scenarios. They may act early to avoid any possible damage, or to assign a new route in case of a traffic accident in the existing route. SPBA makes use of both ECDSA signatures and TESLA-based scheme to authenticate beacons. Similar to the TESLA scheme, SPBA also requires loose time synchronization. In VANETs, it is naturally supported since messages sent by GPS-equipped vehicles are time stamped with nanosecond-level accuracy.

Protocol Overview

SPBA includes the process of generating a signature by a sender and verifying the signature by a receiver. First, each vehicle splits its timeline into a sequence of time frames. Each time frame is also divided into a sequence of beacon intervals, which we remark I_0; I_1; . . . ; In. In a time frame, to send the first beacon B0 for I_0, a vehicle will perform four steps: chained keys generation, position prediction, Merkle hash tree construction, and signature generation.

Sender Side Process

- Chained Keys Generation:

At the beginning of a time frame, each vehicle generates n chained private keys for the next n beacons. It uses one interval worth of private key for authentication as the TESLA scheme. In the following description, we call these private keys TESLA keys.

- Position Prediction:

At each beacon interval, each vehicle predicts its position broadcast in the next beacon. To do so, vehicles model all the possible results of movements between two consecutive beacons based on information of the past trajectory.

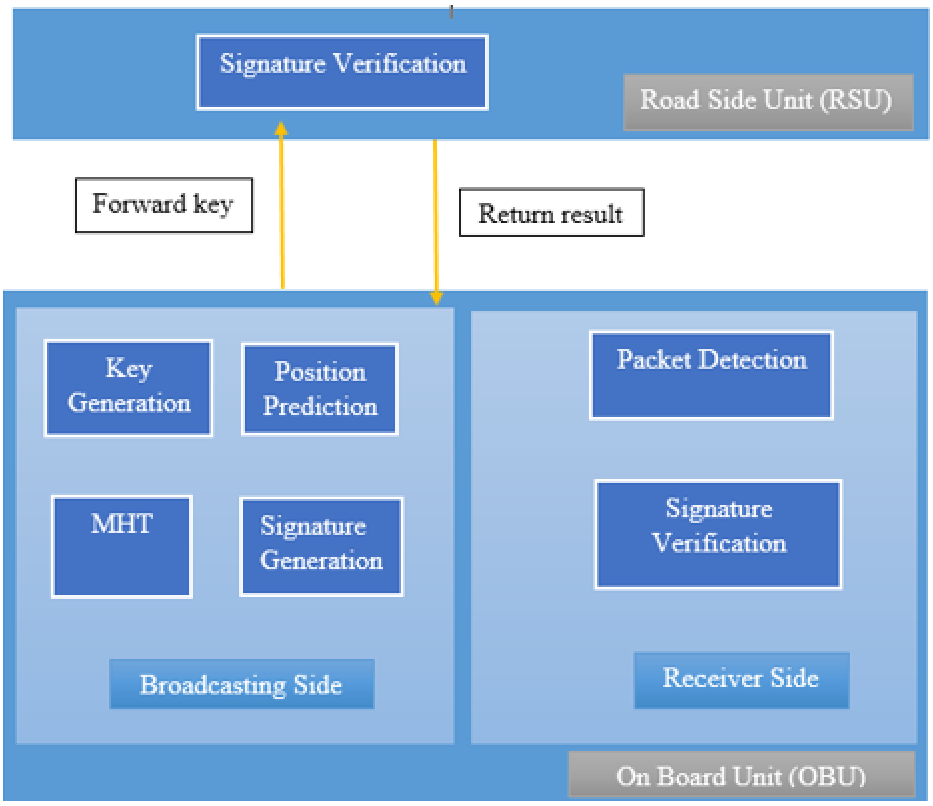

Figure2: System Architecture

- Merkle Hash Tree Construction:

After position prediction, the vehicle will construct one interval worth of a public key and private keys. These private keys are associated with the results of movements. MHT structure is proposed to ties these pre-computed keys together and then generates a single public key or prediction outcome for all the possible movements.

- Signature generation:

After position prediction and MHT construction, a vehicle signs the commitment of the hash chain and the prediction outcome from MHT using ECDSA signatures, and broadcasts it along with the first beacon B0 in the time frame. For the rest of beacons such as B_1; B_2; . . .;B_n, the vehicle signs the message and the prediction outcome from MHT using the TESLA keys assigned in the intervals I_1; I_2;. . . ; In. It contains public keys, time stamp T_0, and other important parameters.

Receiver Side Process

- Attack packet detection:

It is based on the position changing requirements. Attacked packets are identified by the following parameters Frequency (f), Velocity (v), is Coefficient which is determined by the road characteristics and (VMax) is the maximum speed. After receiving a beacon, a vehicle will perform the following two steps:

a) Self-generated MAC storage:

To reduce the storage cost of unverified signatures, the receiver only records a shortened re-keyed MAC. When the receiver keeps the used key secret, SPBA provides security guarantees according to the size of beacon interval and network bandwidth.

b) Signature verification:

For the first beacon, the receiver veryfies the ECDSA signature. To verify the following signed Bi, the receiver will get the corresponding TESLA key, and reconstruct the prediction outcome from MHT. If a matching MAC of prediction outcome is found in the memory, the receiver authenticates the beacon instantly. Otherwise, the receiver authenticates it with the later TESLA key.

VI. CONCLUSIONS

In this paper, we presented some of the most relevant broadcast dissemination schemes specially designed for VANETs, highlighting their features, and studying their performance under the same simulation conditions, thus offering researchers a fair comparison between different broadcast schemes. In particular, we presented a classification of the broadcast dissemination schemes and classified them according to the different characteristics and techniques they use to determine whether a car is allowed to rebroadcast a packet. In addition, we simulated all these schemes by using a real visibility model and under realistic urban environment conditions. According to the results obtained, we observed that Store and forward broadcasting schemes, which account for the beacons received and the map topology, achieve a higher percentage of informed nodes, especially in sparse scenarios. However, when density increases, the high volume of messages produced is prone to saturate the channel. Additionally, we find that, as expected, adaptive dissemination schemes achieve intermediate values, offering a good trade-off between the measured metrics(i.e., informed vehicles, messages received, and warning notification time) for all the vehicle densities studied..

VII. REFERENCES

[1] F. J.Martinez, C.-K. Toh, J.-C. Cano, C. T. Calafate, and P.Manzoni, “Emergency services in future intelligent transportation systems based on vehicular communication networks,” IEEE Intelligent Transportation SystemsMagazine, vol. 2, no. 2, pp. 6–20, 2010.

[2] P. Fazio, F. De Rango, and A. Lupia, “A new application for enhancing VANET services in emergency situations using the WAVE/802.11p standard,” in Proceedings of the IFIP Wireless Days (WD ’13), pp. 1–3, Valencia, Spain, November 2013.

[3] N. Kumar, N. Chilamkurti, and J. J. P. C. Rodrigues, “Learning automata-based opportunistic data aggregation and forwarding scheme for alert generation in vehicular ad hoc networks,”Computer Communications, vol. 39, pp. 22–32, 2014.

[4] K. Shafiee, J. Lee, V. C. M. Leung, and G. Chow, “Modeling and simulation of vehicular networks,” in Proceedings of the 1st ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications (DIVANet ’11), pp. 77–85, ACM, New York, NY, USA, November 2011.

[5] Y.-C. Tseng, S.-Y. Ni, Y.-S. Chen, and J.-P. Sheu, “The broadcast stormproblemin a mobile ad hoc network,” Wireless Networks, vol. 8, no. 2-3, pp. 153–167, 2002.

[6] M. Fogue, P. Garrido, F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni, “Automatic accident detection: assistance through communication technologies and vehicles,” IEEE Vehicular Technology Magazine, vol. 7, no. 3, pp. 90–100, 2012.

[7] M. Fogue, P. Garrido, F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni, “A system for automatic notification and severity estimation of automotive accidents,” IEEE Transactions on Mobile Computing, vol. 13, no. 5, pp. 948–963, 2014.

[8] M. Fogue, P. Garrido, F. J. Martinez, J.-C. Cano, C. T. Calafate, and P.Manzoni, “A novel approach for traffic accidents sanitary resource allocation based on multi-objective genetic algorithms,” Expert Systems with Applications, vol. 40,no. 1, pp. 323– 336, 2013.

[9] P. Ruiz and P. Bouvry, “Survey on broadcast algorithms for mobile ad hoc networks,” ACM Computing Surveys, vol. 48, no. 1, article 8, 2015.

[10] L. Cheng, B. E. Henty, R. Cooper, D. D. Stancil, and F. Bai, “A measurement study of time-scaled 802.11a waveforms over the mobile-to-mobile vehicular channel at 5.9GHz,” IEEE Communications Magazine, vol. 46, no. 5, pp. 84–91, 2008.

[11] S. Panichpapiboon and W. Pattara-Atikom, “A review of information dissemination protocols for vehicular ad hoc networks,” IEEE Communications Surveys and Tutorials, vol. 14, no. 3, pp. 784–798, 2012.

[12] X. Li and H. Li, “A survey on data dissemination in VANETs,” Chinese Science Bulletin, vol. 59, no. 32, pp. 4190–4200, 2014.

[13] J. Harri, F. Filali, and C. Bonnet, “Mobility models for vehicular ad hoc networks: a survey and taxonomy,” IEEE Communications Surveys & Tutorials, vol. 11, no. 4, pp. 19–41, 2009.

[14] D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, “A survey on platoon-based vehicular cyber-physical systems,” IEEE Communications Surveys&Tutorials, vol. 18,no. 1, pp. 263–284, 2015.

[15] S.Madi and H. Al-Qamzi, “A survey on realistic mobility models for vehicular ad hoc networks (VANETs),” in Proceedings of the 10th IEEE International Conference on Networking, Sensing and Control (ICNSC ’13), pp. 333–339, April 2013.

[16] M. S. Al-Kahtani, “Survey on security attacks in vehicular ad hoc networks (VANETs),” in Proceedings of the 6th International Conference on Signal Processing and Communication Systems (ICSPCS ’12), pp. 1–9, Queensland, Australia, December 2012.

[17] H. Al Falasi and E. Barka, “Revocation in VANETs: a survey,” in Proceedings of the International Conference on Innovations in Information Technology (IIT ’11), pp. 214–219,AbuDhabi,United Arab Emirates, April 2011.

[18] F. Li and Y. Wang, “Routing in vehicular ad hoc networks: a survey,” IEEE Vehicular Technology Magazine, vol. 2, no. 2, pp. 12–22, 2007.

[19] H. Keshavarz and R. M. Noor, “Beacon-based geographic routing protocols in vehicular ad hoc networks: a survey and taxonomy,” in Proceedings of the IEEE Symposium on Wireless Technology and Applications (ISWTA ’12), pp. 309–314, IEEE, Bandung, September 2012.

[20] S. Allal and S. Boudjit, “Geocast routing protocols for VANETs: survey and guidelines,” in Proceedings of the 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS ’12), pp. 323–328, IEEE, Palermo, Italy, July 2012.

[21] A. Sebastian, M. Tang, Y. Feng, and M. Looi, “A multicast routing scheme for efficient safety message dissemination in VANET,” in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC ’10), pp. 1–6, Sydney, Australia, April 2010.

[22] F. Soldo, R. Lo Cigno, and M. Geria, “Cooperative synchronous broadcasting in infrastructure-to-vehicles networks,” in Proceedings of the 5th Annual Conference on Wireless on DemandNetwork Systems and Services (WONS ’08), pp. 125–132, Garmisch-Partenkirchen, Germany, January 2008.

[23] F. J. Martinez, J.-C. Cano, C. T. Calafate, P. Manzoni, and J. M. Barrios, “Assessing the feasibility of a VANET driver warning system,” in Proceedings of the 4th ACM Workshop on Performance Monitoring and Measurement of Heterogeneous Wireless and Wired Networks (PM2HW2N ’09), pp. 39–45, ACM, 2009.

[24] G. Y. Cahng, J.-P. Sheu, and J.-H. Wu, “Typhoon: resource sharing protocol for metropolitan vehicular ad hoc networks,” in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC ’10), pp. 1–5, Sydney, Australia, April 2010.

[25] X.Hu, J. Zhao,D. Zhou, andV. C. M. Leung, “Asemantics-based multi-agent framework for vehicular social network development,” in Proceedings of the 1st ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications (DIVANet ’11), pp. 87–96, ACM, New York, NY, USA, November 2011.

[26] S. Samarah, “Grid-based hierarchy structure for mining and querying vehicular ad-hoc networks,” in Proceedings of the Second ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks andApplications (DIVANet ’12), pp. 63–68, ACM, 2012.

[27] J. Jakubiak and Y. Koucheryavy, “State of the art and research challenges for VANETs,” in Proceedings of the 5th IEEE Consumer Communications and Networking Conference (CCNC’08), pp. 912–916, Las Vegas, Nev, USA, January 2008.

[28] DoT, “United States Department of Transportation,” 2015, http://www.dot.gov/.

[29] Z. Movahedi, R. Langar, and G. Pujolle, “A comprehensive overview of vehicular AdHocNetwork evaluation alternatives,” in Proceedings of the 8th Asia-Pacific Symposium on Information and Telecommunication Technologies (APSITT ’10), pp. 1–5, Kuching, Malaysia, June 2010.

[30] A. J. Ghandour, M. Di Felice, H. Artail, and L. Bononi, “Dissemination of safetymessages in IEEE 802.11p/WAVE vehicular network: analytical study and protocol enhancements,” Pervasive and Mobile Computing, vol. 11, pp. 3–18, 2014.

[31] J.Dias, J. Rodrigues, J. Isento, and J. Niu, “The impact of cooperative nodes on the performance of vehicular delaytolerant networks,” Mobile Networks and Applications, vol. 18, no. 6, pp.867–878, 2013.

[32] J. N. G. Isento, J. J. P. C. Rodrigues, J. A. F. F. Dias, M. C. G. Paula, and A. Vinel, “Vehicular delay-tolerant networks? Anovel solution for vehicular communications,” IEEE Intelligent Transportation Systems Magazine, vol. 5, no. 4, pp. 10–19, 2013.

[33] P. R. Pereira, A. Casaca, J. J. P. C. Rodrigues, V. N. G. J. Soares, J. Triay, and C. Cervell´o-Pastor, “From delay-tolerant networks to vehicular delay-tolerant networks,” IEEE Communications Surveys and Tutorials, vol. 14, no. 4, pp. 1166–1182, 2012.

[34] Q. Chen, D. Jiang, and L. Delgrossi, “IEEE 1609.4 DSRC multichannel operations and its implications on vehicle safety communications,” in Proceedings of the IEEE Vehicular Networking Conference (VNC ’09), pp. 1–8, Tokyo, Japan, October 2009.

[35] Q.Xu, T.Mak, J. Ko, andR. Sengupta, “Vehicle-to-vehicle safety messaging inDSRC,” in Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET ’04), pp. 19–28, ACM, NewYork, NY,USA, 2004.

[36] Q. Xu, T. Mak, J. Ko, and R. Sengupta, “Medium access control protocol design for vehicle—vehicle safety messages,” IEEE Transactions on Vehicular Technology, vol. 56, no. 2, pp. 499–518, 2007.

[37] M. Torrent-Moreno, P. Santi, and H. Hartenstein, “Fair sharing of bandwidth in VANETs,” in Proceedings of the 2nd ACM International Workshop on VehicularAdHoc Networks (VANET ’05), pp. 49–58, New York, NY, USA, 2005.

[38] F. Farnoud and S. Valaee, “Repetition-based broadcast in vehicular ad hoc networks in Rician channel with capture,” in Proceedings of the IEEE INFOCOM Workshops, pp. 1–6, Phoenix, Ariz, USA, April 2008.

[39] B. Hassanabadi and S. Valaee, “Reliable periodic safety message broadcasting in VANETs using network coding,” IEEE Transactions on Wireless Communications, vol. 13, no. 3, pp. 1284–1297,2014.

[40] Y. Park and H. Kim, "Collision control of periodic safety messages with strict messaging frequency requirements," IEEE Transactions onVehicular Technology, vol. 62,no. 2, pp.843–852, 2013.

[41] [N. Wisitpongphan, O. K. Tonguz, J. S. Parikh, P. Mudalige, F. Bai, and V. Sadekar, "Broadcast storm mitigation techniques in vehicular ad hoc networks," IEEEWireless Communications, vol. 14, no. 6, pp. 84–94, 2007.

[42] K. Suriyapaibonwattana and C. Pomavalai, "An effective safety alert broadcast algorithm for VANET," in Proceedings of the International Symposium on Communications and Information Technologies (ISCIT '08), pp. 247–250,Vientiane, Laos, October 2008.

[43] K. Suriyapaiboonwattana, C. Pornavalai, and G. Chakraborty, "An adaptive alert message dissemination protocol for VANET to improve road safety," in Proceedings of the IEEE International Conference on Fuzzy Systems (FUZZ-IEEE '09), pp. 1639–1644, Jeju Island, Republic of Korea, August 2009.

[44] M. Slavik and I. Mahgoub, "Stochastic broadcast for VANET," in Proceedings of the 7th IEEE Consumer Communications and Networking Conference (CCNC '10), pp. 1–5, IEEE, Las Vegas, Nev, USA, January 2010.

[45] F. J.Martinez, M. Fogue, M. Coll, J.-C. Cano,C.Calafate, and P. Manzoni, "Evaluating the impact of a novel warning message dissemination scheme for VANETs using real city maps," in NETWORKING 2010: 9th International IFIP TC 6 Networking Conference, Chennai, India, May 11–15, 2010. Proceedings, M. Crovella, L. Feeney, D. Rubenstein, and S. Raghavan, Eds., vol. 6091 of Lecture Notes in Computer Science, pp. 265–276, Springer, Berlin, Germany, 2010.

[46] M. Fogue, P. Garrido, F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni, "Evaluating the impact of a novel message dissemination scheme for vehicular networks using real maps," Transportation Research Part C: Emerging Technologies, vol. 25, pp. 61–80, 2012.

[47] F. J. Ros, P. M. Ruiz, and I. Stojmenovic, "Reliable and efficient broadcasting in vehicular ad hoc networks," in Proceedings of the IEEE 69th Vehicular Technology Conference (VTC Spring '09), pp. 1–5, IEEE, April 2009.

[48] C. Sommer, O. K. Tonguz, and F. Dressler, "Traffic information systems: efficient message dissemination via adaptive beaconing," IEEE CommunicationsMagazine, vol. 49,no. 5, pp. 173–179, 2011.

[49] Y. Bi, L. X. Cai, X. Shen, and H. Zhao, "A cross layer broadcast protocol for multihop emergency message dissemination in inter-vehicle communication," in Proceedings of the IEEE International Conference on Communications (ICC '10), pp. 1–5, Cape Town, South Africa, May 2010.

[50] J. A. Sanguesa, M. Fogue, P. Garrido et al., "On the selection of optimal broadcast schemes in VANETs," in Proceedings of the 16th ACM International Conference on Modeling, Analysis and Simulation ofWireless andMobile Systems(MSWiM'13), pp.411–418, Barcelona, Spain, November 2013.

[51] J. A. Sanguesa, M. Fogue, P. Garrido, F. J. Martinez, J.-C. Cano, and C. T. Calafate, "Topology-based broadcast schemes for urban scenarios targeting adverse density conditions," in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '14), pp. 2528–2533, IEEE, Istanbul, Turkey, April 2014.

[52] J. A. Sanguesa, M. Fogue, P. Garrido, F. J. Martinez, J.-C. Cano, and C. T. Calafate, "Using topology and neighbor information to overcome adverse vehicle density conditions," Transportation Research Part C: Emerging Technologies, vol. 42, pp. 1–13, 2014.

[53] S.-I. Sou and Y. Lee, "SCB: store-carry-broadcast scheme for message dissemination in sparse VANET," in Proceedings of the IEEE 75thVehicular Technology Conference (VTC Spring '12), pp.1–5, IEEE, Yokohama, Japan, May 2012.

[54] O. K. Tonguz, N. Wisitpongphan, and F. Bai, "DV-CAST: a distributed vehicular broadcast protocol for vehicular ad hoc networks," IEEEWireless Communications, vol. 17, no. 2, pp. 47– 57, 2010.

[55] W. Viriyasitavat, O. K. Tonguz, and F. Bai, "UV-CAST: an urban vehicular broadcast protocol," IEEE CommunicationsMagazine, vol. 49, no. 11, pp. 116–124, 2011.

[56] D. Sormani, G. Turconi, P. Costa, D. Frey, M. Migliavacca, and L.Mottola, "Towards lightweight information dissemination in inter-vehicular networks," in Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks (VANET '06), pp. 20– 29, ACM, Los Angeles, Calif, USA, September 2006.

[57] J. A. Sanguesa, M. Fogue, P. Garrido et al., "RTAD: a realtime adaptive dissemination system for VANETs," Computer Communications, vol. 60, pp. 53–70, 2015