Inter vehicular communication by fast and secure multihop broadcasting to ensure security of communication

Shweta A.Ingle[1], Prof. Manjiri U.Karande[2]

[1] Post Graduate Student, Department of CE, Padm.Dr. V.B.K.C.O.E., Malkapur, S.G.B.A. University, Maharashtra, India

[2] Asst. Professor, Department of CSE, Padm. Dr. V.B.K.C.O.E., Malkapur, S.G.B.A. University, Maharashtra, India

[1]pshweta102@gmail.com

[2]manjiri.karande@gmail.com

***Abstract*— Inter vehicular communication (IVC) is an important to transpire investigate area that is look for to greatly subscribe to traffic safety and efficiency. For fast multihop message spread, containing information such as position, track and speed allotted the usual need by a lot of probable IVC application. It is critical for such a data exchange system to be flexible to security attack. Contrary, a harmful vehicle might introduce incorrect information in to the inter vehicle wireless links, essential to life and money losses or to any other sort of enemy egotism. (e. g. traffic turns for the adversarial benefit). They analyze essential us to design a fast and secure multihop broadcast algorithm for inter vehicular communication, which is demonstrate to be flexible to the previously attacks.**

I. INTRODUCTION

INTERVEHICULAR COMMUNICATION (IVC) is among the most capable and demanding application of vehicular ad hoc networks (VANETs) [2], [3]. Many applications are probable in this context, up till now local danger warning systems remain the most famous ones. Most of these safety-related applications, with up to date ones, contribute to property that place them into the similar group of solutions: IVC-based vehicular safety applications [4]–[7]. These general properties are listed as follows.

1) Communication is commonly vehicle-to-vehicle (V2V), with no infrastructure.

2) Vehicles replace messages that include their position , direction, speed, and possible dangers.

3) Broadcast messages include to be propagating as quickly as possible in a sure area of interest, even though multihop forwarding.

4) Specific algorithms are employed to decide as few forwarders as possible over the multihop path to fasten the propagation of alert messages.

5) Vehicles' information such as position, track, speed and transmission range is use to provide for the forwarder selection algorithm.

Obviously, the effectiveness of such a safety-related application is base on the consistency of broadcast information. To talk about attacks to IVC-based safety applications, we consider a state of- the-art protocol that is delegate of this class of applications: the fast multihop broadcast algorithm (FMBA) [3]. for the reason that the attacks and solutions depend on the above mentioned five properties (also overcome by FMBA), FMBA allows us to make clear the explanation appropriate to a practical case study, up till now with no loss of majority. Contribution. During the use of a representative case study, we evaluate the security threats to up to date IVC-based safety applications that as well propose counter trial for these threats. That's why we propose a solution that is together fast and secure within broadcasting safety-related messages: fast and secure multihop broadcast algorithm (FS-MBA).

II. LITERATURE SURVEY

Since, the evolution of VANETs various techniques and concepts have been used in order to overcome the problems while propagating security alerts or emergency warning message IVC is an main component of the intelligent transportation system [2],[8]–[10]. Information that is collected from IVC can short-term road safety and transportation efficiency. Benefiting from the large bulks (in terms of both space and power) of vehicles, the nodes of these networks can take long transmission ranges and infinite lifetimes. The main IVC application scan be considered into the following three classes [6].

1. Information and notice functions: Distribution of road information (with accidents and road congestion) to remote vehicles2. Communication-based longitudinal control: Developing the" look-through" ability of IVC to help avoid accidents.

3. Supportive assistance system: Coordinating vehicles at dangerous points such as blind crossing (a crossing with no light control) and highway entry.

A. Routing within Vehicular Networks

Due to high flexibility, effective routing represent a critical technical challenge within vehicular communications, thus attracting the care of researchers [9], [11], [12]. In overall, topology routing protocols use the connection state in the network to transmit the packet from the source to the destination, while this approach would fail in the occurrence of highly variable connectivity between nodes. For the reason that vehicular communication can contract with not only a large number of vehicles but also with interest for resident information, geographical routing may represent an efficient approach [11]. Routing that is support on geographic location exploit nodes' knowledge almost their position and

their neighbors' location, which is found through services such as the Global position System (GPS).Forwarding decisions are

B. Fast Broadcast within Safety Applications

A number of IVC applications need multihop broadcast update vehicles (and drivers) about road data, transport announcements, traffic congestion, closeness with other vehicles, accidents, and entertainment associated information [4]–[7], [13]. The simplest broadcasting mechanism is overflowing, wherever messages are rebroadcast by every receiving node. Even though very simple, this technique may lead to high message crash chance and data redundancy, thus becoming somewhat inefficient. When a message is distributed to receivers out there the transmission range, multi hopping could be used. On the other hand, multihop broadcast can consume a significant amount of wireless resources designed for redundant retransmissions. The broadcast delivery time denotes one of the main matters of IVC. It has been prove that this feature is strictly related to both the number of relays of the messages (hops) and the network congestion [4], [5], [7], [14]–[15].The demand-driven broadcast protocol modifies the timing of rebroadcast packets such that the vehicle that is farthest away since the source node retransmits previous than the other nodes [14]. Ad hoc multihop broadcast and town multihop broadcast are planned in [7] for vehicular networks. These protocols are planned to address the broadcast storm, hidden node, and reliability problems in multihop broadcast. Sender nodes try to choose the farthest node in the broadcast track to assign the function of forwarding and acknowledging the packet without any a prior topology information. FMBA aims at reducing the number of hops that were traversed by a message to minimize the broadcast delay of a message [4]. Vehicles in a car platoon dynamically estimate their transmission range and use this information to powerfully spread a broadcast message with as few transmissions as possible. In essence, the farthest vehicle in the transmission series of a message sender or forwarder will statistically be advantaged in appropriate theater that (and only) forwarder. In [5], this algorithm was improved, considering heterogeneous transmission range; the message forwarder becomes the vehicle within the transmission range with the farthest distance, rather than the farthest vehicle. In review, several multihop broadcast algorithms have been planned. Unfortunately, they have all been developed with no safety in mind, whereas security is a fundamental problem in this context that should not be unnoticed [16].Indeed, attackers may run malicious actions to insert false information or alarm, thus exposé the protection application unsuccessful [17]–[18].In more detail, in, the attack on vehicular communications were categorize as follow.

1. Bogus information. One or several rightful members of the network send out false information to misguide new vehicles concerning traffic conditions. To manage with such misconduct, the received data from a given source should be

in use base on the geographical locations of neighbors and of the target. Geographic routing protocols are not necessary to keep up explicit routes, therefore scaling well even using dynamic networks.

confirmed by correlate and comparing them with the data received from further sources.

2. Wrong on positioning information. Insertion of a fake location by a malicious vehicle that pretend to be at a claim location.

3. ID exposé of other vehicles. This is to path their place. A global body can check trajectory of under attack vehicles and use these data for a lot of purpose, and we could get the pattern of some car rental companies that path their individual cars.

4. Denial of Service (DoS). The attacker might wish for to transport down the IVC or still cause an accident. Example of attacks contains channel congestion and violent inoculation dummy messages.

5. Masquerade. The attacker claim to be one more vehicle by with fake identities. We highlight on one of the major threats to security application: the risk of attacking the protocol to impede its helpful service. For easiness of exhibition but with no loss of generalization, we mainly focus on FMBA, for the reason that it embody both a up to date solution and a delegate example of the IVC-based vehicular security applications class possessing all the five property mention in Section I. Certainly, harms and probable counter events that were identified for FMBA can also be modified to other protocols/algorithms that fit in to the same common class of applications distribution the above mention set of property. Lastly, security that is accessible in infrastructure-based multicast otherwise transmits, such as in WiMax and other parallel wireless technologies (e.g., [19]), could be considering for service, still in vehicular networks. Furthermore, several result are focused on broadcast base on fixed network with pre recognized common secrets among nodes and the base station ,thus introduce delays [20]. Unfortunately, the unusual size, mobility, and connectivity of vehicular networks build the abovementioned solutions not appropriate for this background. Furthermore, road-safety-related applications are harshly based on geographic area and on real-time reply, thus achieving higher effectiveness level when based on V2V communication somewhat than resorting on central approach.

III. Related Work

We show the notation (review in Table I) and assumption used in this paper. Also, we explain FMBA—the case study selects to represent IVC-based vehicular security applications—in detail. Note that FMBA is planned to speed up multihop broadcast both forward and backward. Though, for clearness, we submit only to the case wherever alert messages have to be send only backward through the vehicular traveling track (the forward case is just secular).

A. Model Assumptions

To make simpler the conversation, we have completed the following assumption about the general model that we are allowing for. We assume that at mainly one malicious vehicle is on top of the network. There are no obstacle and no building in the road. The investigation communication series is symmetric. It means so as to, if a vehicle V hear a vehicle P, and then we suppose that P can too hear V. We assume that there are N vehicles approved in the section. A section can be look at as a collection of nodes/vehicles that are linked by a wireless local area network and are engage in longitudinally next each other. A vehicle V do not knows its transmission range. The verifier node V straight communicates with the confirmed node P. Each vehicle know its personal position, e.g., using GPS, which provide correct information regarding time and location.

Symbol	Definition
CMBR	Current Maximum Back Range
CMFR	Current Maximum Front Range
LMBR	Latest -Turn Maximum Back Range
LMFR	Latest -Turn Maximum Front Range
Max Range	How far the transmission is expected to go backward before the signal becomes not strong to be intelligible.
D	Distance between two vehicles
CW	Connection Window
CW Max	Maximum Connection Window
CW Min	Minimum Connection Window
Hello	Hello message transmitted by a vehicle in the estimation phase to renew the transmission range
Drm	Declared transmission range in the Hello message
P	The prover vehicle
V	The verifier vehicle
R	The geographical region

All the vehicles be in the right place to a public key infrastructure (PKI) [21], [22]; i.e., every vehicle has a public/private couple of keys and a single identity certified by a documentation authority. We suppose that the certification power correspond to the government agency that is accountable for assigning license plates: a vehicle can be used simply if it is provide with a single license plate, a PKI documentation that is linked to its plate ID, and the public key of the certification power. We suppose that certificate revocation list are simplified at a particular time interval (e.g. daily) by the vehicle and store in a local memory. The power and computational resources are imaginary mainly adequate for our application's necessities. The network is insecurely time synchronize.

TABLE I: NOTATION

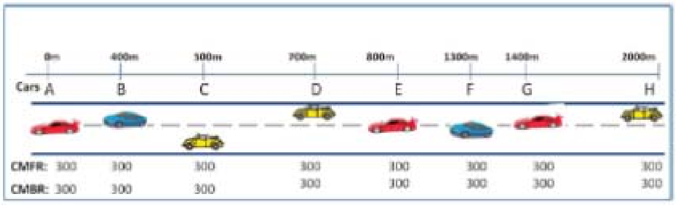
B. FMBA

The plan of FMBA is to decrease the time that is necessary by a message to spread from the source to the farthest vehicle in a sure area of interest [4]. To complete this aim, FMBA exploit a spread mechanism for the judgment of the communication range of vehicles. These communication range estimation are obtain by

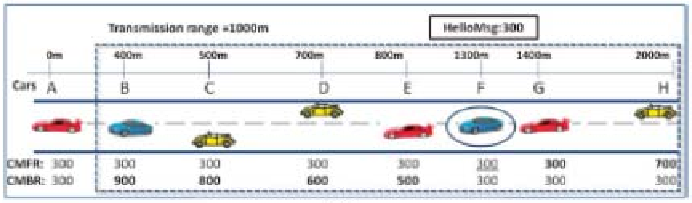
exchange a amount of Hello messages along with the vehicles and are then use to decrease the number of jump that an alert message has to pass through to cover a sure area of interest. This lead to a reduce in the amount of transmissions and the time that is essential by a broadcast message to enter at all the cars that follow the sender in a definite distance. This system is composed of the track two stages: 1) the estimation stage and 2) the broadcast stage. The former phase is constantly active and is meant to give each vehicle with an advanced estimation of its transmission range. The latter phase is performing only after a message has to be transmitting to all vehicles in the sender's region of interest. To forward a packet, each recipient has to calculate its waiting time before attempt to forward the message. This waiting time is expressed throughout a contention window (CW), which is compute using

$$CW = \left| \frac{(MaxRange-d)}{MaxRange} * (CW\ Max - CW\ Min) + CW\ Min \right| \tag{1}$$

When a car has to throw or forward a transmit message, it compute the MaxRange value in the transmit message as the most between LMBR and CMBR values. To keep away from unnecessary transmissions, all vehicles between the original sender and the present forwarder terminate their attempt to forward he message, whereas all vehicles behind the current forwarder calculate a new CW for the next hop. We present the CW computed by dissimilar vehicles through (1). The beyond a vehicle is as of the source of transmit message, the smaller its CW becomes. The waiting time is a value that is at random compute within CW. If we suppose distance among vehicles as d(D, V) ≥d(C, V) ≥d(B, V) ≥d(A, V), after that the vehicles' CWs generate by FMBA becomes CW(D) ≤CW(C) ≤CW(B) ≤CW(A). Therefore, in the considered example, D has the maximum possibility to become the next forwarder, because its waiting time is randomly selected within the minimum CW between those assigned by FMBA to A,B, C, and D.



(a)



(b)

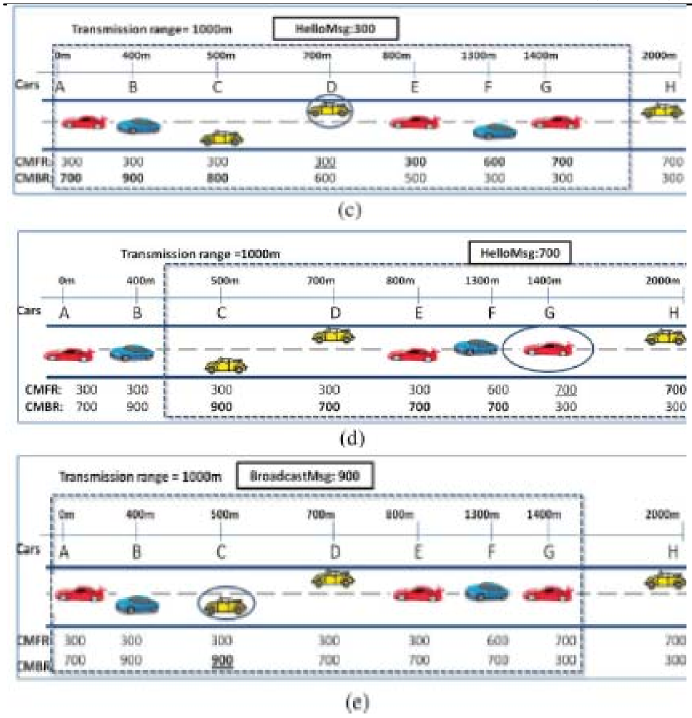

Transmission range= 1000m
HelloMsg:300
0m 400m 500m 700m 800m 1300m 1400m 2000m
Cars A B C D E F G H
CMFR: 300 300 300 300 300 600 700 700
CMBR: 700 900 800 600 500 300 300 300
(c)
Transmission range =1000m
HelloMsg:700
0m 400m 500m 700m 800m 1300m 1400m 2000m
Cars A B C D E F G H
CMFR: 300 300 300 300 300 600 700 700
CMBR: 700 900 900 700 700 700 300 300
(d)
Transmission range = 1000m
BroadcastMsg: 900
0m 400m 500m 700m 800m 1300m 1400m 2000m
Cars A B C D E F G H
CMFR 300 300 300 300 300 600 700 700
CMBR 700 900 900 700 700 700 300 300
(e)

Fig. 1. (a) Initial state. (b) First Hello Message. (c) Second Hello message. (d) Third Hello message. (e) Broadcast message. [1]

ATTACK 1: POSITION-CHEATING ATTACK

A malicious node could broadcast in a Hello message a fake position that is more far-away than the real one. Then, direct nodes that finally receive an alert broadcast message will calculate unnecessarily large CWs, thus slow down the forward process. For ease of appearance show the impact of this attack that information the CWs of some vehicles, depending on their detachment from the original sender/forwarder (vehicle V) of the aware message. In particular, since the CW of each vehicle is computed through (1), with no any malicious vehicle, the function should differ (from its most in correspondence of vehicle V to its least at the end of the transmission series, which i s assumed to be close to vehicle D). In its place, if through the estimation phase, a malicious vehicle within V's transmission range send a Hello message to declare a fake position that correspond to M, the transmission range judgment of vehicle V would incorrectly be compute as the distance from V to M, in its place of from V to D. These lead vehicles A, B, C, and D to miscalculate their CWs, because they will think the minimum CW in position M. This easy up till now effective attack modify the calculation of CW, increasing the average contention time of each node previous to any forwarding transmission can get place, hence slowdown the transmission of the aware message.

ATTACK 2: REPLAY BROADCAST MESSAGE ATTACK

In this situation, we think a direct node that broadcasts a message to the entire receiver in its broadcast range. We suppose that the adversary intercept the broadcast message and rebroadcasts it with no waiting. primary, we comment that, for all the nodes that collect this same broadcast message from the front, the attacker push them to resume the broadcast process (as explain in the forward process of a broadcast message).Second, all the nodes that obtain delivery of this message from the backstop trying to forward this message. In fact, according to FMBA, the messages have been propagate over the consider vehicles, and these vehicles will way out the forwarding procedure. The challenger could repeat broadcasting the similar message, pushing the nodes to not forward the packet by now restarting at every time the broadcast procedure. The honest car (C) forwards its messages. In this attack situation, we assume that the vehicle (M) is hateful and does not stay for the finishing of its time space; it instantly sends the message. while in receipt of the message, vehicles that are behind M restart the broadcast procedure, while nodes that are in front of M will leave the forwarding procedure. A malicious node M could do the following operations.1) Modes not adjust the message but just broadcasts it.

1) Nodes previous restarts the forwarding procedure, therefore wasting time.

2) Nodes in front of M exit the forwarding procedure. No one could forward the packet if the opponent repeats every message that is send by the sender (or forwarder).

3) Modify the broadcast message and forwards it through a high MaxRange to generate slow-forwarding hops through vehicles that employ without cause high CWs.

4) M forwards the message with a low MaxRange to add to the possibility that more than one vehicle concurrently attempts to forward the message, therefore result in gin transmit crash and delay.

ATTACK 3: INTERRUPTING A FORWARDING ATTACK

In this situation, the forwarder vehicle is malicious and tries to broadcast a message forward but not backward. To carry out so, the malicious node has to be located at the end of the transmission series and be able with a directional transmitter. By forwarding the alert message only forward, vehicles in front of the malicious node will terminate their forwarding procedure; because the message has been send farther than their location. On the Other hand, vehicles following the malicious node will now not receive any message. Let us consider the attack scenario depicted in Fig. The direct vehicle C broadcasts a message, while the forwarder vehicle is M, which maliciously forwards the message only frontward. Vehicles (D, E, and F) will therefore exit the forwarding process and the forwarded message will not at all be propagate toward next cars. Furthermore, malicious nodes may work together to block the transmission of messages in n zones.

SOLUTION TO ATTACK 1:
FALSE-POSITION DETECTION

In this section, we explain our position verification system. Our solution requires no infrastructure but only distributed messages that are exchanged between nodes to sense the malicious nodes. In reality, we thrash out how the information of the vehicles could be propagating to other vehicles to have a total and a local inspection. First, we converse the structure of the transmit message and the timing of forwarding or transmit the information. Next, these data might be collect from through neighbors (in case nodes openly communicate) or from multihop neighbors (in case of circumlocutory or asymmetric communication) between vehicles. However, we should bound the multihop spread of this information in a limited area. Collected information should be fresh and limited to the participate nodes. Third, to guarantee the validity of messages, nodes carry on to an authentication mechanism. To perform this, we suggest transmitting the information of vehicles in an adapted Hello message. We present the transfer and getting procedure of Hello message. Once getting the different reports (the modified Hello messages) from vehicles, every verifier nearby executes a position verification process. Then, the verifier vehicle could notice whether the claim position of a vehicle M is fake.

SOLUTION TO ATTACK 2: ANTIREPLAY PROTECTION

In this part, we give a complete description of our proposed solution for detect malicious vehicles base on message replace. To this plan, we talk about the structure of the broadcast message and they require for a store table to detect replay messages. In addition, to assurance the authenticity of messages, nodes carry on to a verification mechanism. We broadcast the timestamp in the broadcast message and to store up in each vehicle a table that contains the last previous transmit broadcast messages. We present the distribution and the getting procedure of a broadcast message. Later than receiving the broadcast Messages of a forwarder vehicle, a recipient of the message nearby executes a verification process. Then, this vehicle could notice whether the transmit message is a replay message. The verifier vehicle uses the information store in its table and the forward time to decide whether it is our play broadcast message.

SOLUTION TO ATTACK 3: INTERRUPTING FORWARDING ATTACK DETECTION

In this segment, we detail the transmission of a receipt message through a forwarder vehicle, as well as the authentication that is performing by the verifier node.1) Receipt Message: To throw an evidence of packet relay, the forwarder vehicle has to generate a receipt message. In detail message that contain the vehicle_id, the vehicle position, the timestamp, and an autograph that is generate by the forwarder private key. The verifier node collect authenticated gate (having the vehicle uniqueness, timestamp, and the receipt message), and perform some verifications to identify possible malicious forwarders trying to end the spread of forwarders make contact with the verifier node at smallest amount once through each time interval to send their receipts. Following forwarding a transmit message, the forwarder sends to the verifier node a receipt message that contain the vehicle_id, the vehicle position, the timestamp, and an autograph that is generated by the forwarder private key. The verifier node collect valid receipts (containing the vehicle uniqueness, timestamp, as well as the receipt message), and Performa few verifications to detect probable malicious forwarders trying to end the spread of the transmit message.

TABLE 2 OVERVIEW OF ATTACKS

Attack on FMBA	State of the art solutions	Our proposed solution	Class of Attack[ ]
Position cheating	Infrastructure, parameter, and Model based approaches.	Infrastructure –less and cooperative neighbors technique.	Cheating on positioning information; Denial of Service.
Replay broadcast message	Selfish behavior, replay and duplicate message detections and preventions.	Storing the information broadcast message for a certain period to avoid its transmission by another node.	Denial of Service.
Interrupting forwarding	Reputation or credit based approaches.	Malicious node behavior detection based on receipt messages as a proof of forwarding alert messages.	Denial of Service.

IV. CONCLUSION

The major aim of IVC consists of growing people's security by exchange warning messages between vehicles. It has scratched the plane of what is hopeful to be a new and productive area of research in IVC security. We have study on security issues in IVC, allowing for a general class of applications base on multihop transmit; we have selected a delegate case study for this class, FMBA, to concretely talk about issues and solutions. we have provide an general idea of the different attacks and safety weaknesses, also propose possible countermeasures.

REFERENCES

[1] Wafa Ben Jaballah, Mauro Conti, Mohamed Mosbah, and Claudio E. Palazzi," Fast and Secure Multihop Broadcast Solutions for Intervehicular Communication," IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 15, NO. 1, FEBRUARY 2014

[2]M. L. Sichitiu and M. Kihl, "Intervehicle communication systems: A survey," IEEE Commun. Surveys Tuts., vol. 10, no. 2, pp. 88–105, 2nd Quart., 2008.

[3]C. Wu and Y. Liu, "Queuing network modeling of driver workload and performance," IEEE Trans. Intell. Transp. Syst., vol. 8, no. 3, pp. 528– 537, Sep. 2007.

[4]C. E. Palazzi, S. Ferretti, M. Roccetti, G. Pau, and M. Gerla, “How do you quickly choreograph intervehicular communications? A fast vehicle-tovehicle multihop broadcast algorithm, explained,” in Proc. IEEE CCNC, Jan. 2007, pp. 960–964.

[5]A. Amoroso, M. Ciaschini, and M. Roccetti, “The farther relay and oracle for VANET: Preliminary results,” in Proc. IEEE WICON, 2008, pp. 1307–1311.

[6]J. Luo and J.-P. Hubaux, A Survey of Research in Intervehicle Communications. New York, NY, USA: Springer-Verlag, 2006, pp. 111–122, Embedded Security in Cars–Securing Current and Future Automotive IT Applications.

[7]G. Korkmaz, E. Ekici, F. Özgüner, and Ü. Özgüner, “Urban multihop broadcast protocols for intervehicle communication systems,” in Proc. ACM Workshop VANET, Oct. 2007, pp. 76–85.

[8]L. Li, J. Song, F.-Y. Wang, W. Niehsen, and N. Zheng, “New developments and research trends for intelligent vehicles,” IEEE Intell. Syst., vol. 20, no. 4, pp. 10–14, Jul./Aug. 2005.

[9]F. Qu, F.-Y. Wang, and L. Yang, “Intelligent transportation spaces: Vehicles, traffic, communications, and beyond,” IEEE Commun. Mag., vol. 48, no. 11, pp. 136–142, Nov. 2010.

[10]T. L. Willke, P. Tientrakool, and N. F. Maxemchuk, “A survey of intervehicle communication protocols and their applications,” IEEE Commun. Surveys Tuts., vol. 11, no. 2, pp. 3–20, 2nd Quart., 2009.

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

[12]Y.-W. Lin, Y.-S. Chen, and S.-L. Lee, “Routing protocols in vehicular ad hoc networks: A survey and future perspectives,” J. Inf. Sci. Eng., vol. 26, no. 3, pp. 913–932, May 2010.

[13]A. Broggi, P. Cerri, S. Ghidoni, P. Grisleri, and H. G. Jung, “A new approach to urban pedestrian detection for automatic braking,” IEEE Trans. Intell. Transp. Syst., vol. 10, no. 4, pp. 594–605, Dec. 2009.

[14]M.-T. Sun, W.-C. Feng, K. Fujimura, T.-H. Lai, H. Okada, and K. Fujimura, “GPS-based message broadcasting for intervehicle communication,” in Proc. ICPP, Aug. 2000, pp. 279–286.

[15]T.-S. Dao, K. Y. K. Leung, C. M. Clark, and J. P. Huissoon, “Markovbased lane positioning using intervehicle communication,” IEEE Trans. Intell. Transp. Syst., vol. 8, no. 4, pp. 641–650, Dec. 2007.

[16]P. Papadimitratos, L. Buttyan, T. Holcze, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, “Secure vehicular communication systems: Design and architectures,” IEEE Commun. Mag., vol. 46, no. 11, pp. 100–109, Nov. 2008.

[17]A. Weimerskirch, J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, “Data security in vehicular communication networks,” in VANET: Vehicular Applications and Internetworking Technologies, K. P. Laberteaux, Ed. Chichester, U.K.: Wiley, Nov. 2009, ch. 9.

[18]Q. Wu, J. Domingo-Ferrer, and Ú. González-Nicolás, “Balanced trustworthiness, safety and privacy in vehicle-to-vehicle communications,” IEEE Trans. Veh. Technol., vol. 59, no. 2, pp. 559–573, Feb. 2010.

[19]G. Kambourakis, E. Konstantinou, and S. Gritzalis, “Revisiting WiMAX MBS security,” J. Comput. Math. Appl., vol. 60, no. 2, pp. 217–223, Jul. 2010.

[20]W. B. Jaballah, M. Mosbah, and H. Youssef, “Performance evaluation of key disclosure delay based schemes in wireless sensor networks,” in Proc. IEEE PERCOM/PERSENS, Mar. 2013, pp. 566–571.

[21]W. Diffie and M. E. Hellman, “New directions in cryptography,” IEEE Trans. Inf. Theory, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[22]R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” ACM Commun. Mag., vol. 21, no. 2, pp. 120–126, Feb. 1978.