ACKNOWLEDGED SECURE DATA DISSEMINATION IN VANET

M. Banupriya[*]

R. Sundaraguru[*]

Abstract— VANET – Vehicular Ad-hoc Network is used for various purposes like driver assistance and car safety, infotainment for passengers, also can get local information such as car parking, fuel prices etc., also for car maintenance. Since it provides various advantages to the drivers and passengers we must consider the security of this system. So the information passing between these vehicles must be reliable. Many protocols exist to solve this problem. One of the protocols ABSM – Acknowledged Broadcast from Static to highly Mobile protocol is proposed for efficient and reliable broadcasting in Vehicular Ad Hoc Network. It reduces redundant transmission and it suitable for all kinds of roads. Here CDS-NES technique is used to form the network and broadcasting the messages. The drawback is it does not deal with multiple transmissions simultaneously. Our proposed system uses Position Aware Reliable Broadcasting Protocol to broadcast the message in the network. Based on the position and velocity of the neighbor it selects the neighbors and broadcast the message. Even if failure happens nearest neighbor will starts the transmission. Acknowledgement will piggybacked with the beacon messages.RSA Algorithm is used to generate the key for packet transmission.

Keywords— Vehicular networks, data dissemination, broadcasting, key Generation, Authentication.

[*] Member IEEE

I. INTRODUCTION

Vehicular ad-hoc networks (VANETs) have started to receive increasing interest recently due to their potential to be used in traffic and safety applications in the upcoming years. In such an ad hoc network, vehicles equipped with a wireless transmission device can send and receive messages at significantly higher speeds compared to traditional mobile ad-hoc networks. Vehicles exchange traffic information as they move through the network, which allows drivers to adjust their routes to avoid congestion, obtain road-condition warnings, and be warned in advance for potential traffic accidents.

While the majority of recent research focused on medium access control and routing protocols with the goal of handling the dynamic behavior of VANETs, an important aspect that needs to be considered is the security in transmitting messages.

M.Banupriya is with the PSN College of Engineering & Technology, Tirunelveli, TN 627152 IND phone: 7708829595; e-mail: priya15701@ gmail.com.

R.Sundaraguru, Professor/Head, was with Department of Electronic and communication, PSN College of Engineering and Technology, Triunelveli, TN 627152 IND.

Manuscript received Mar03, 2013; this work was submitted in International Journal of Engineering, science and Mathematics.

.Security of VANETs is critical in preventing collisions and thus minimizing the risk for major accidents. For instance, all safety-related messages sent by a vehicle must be verified by the recipient for its authenticity and integrity in face of adversaries that may inject messages containing bogus information to the network. Yet the privacy of the driver sending those safety-related messages against unauthorized observers must be guaranteed.

However, this anonymity service should be made conditional, meaning it can be revoked for law enforcement purposes whenever necessary. Besides those aforementioned requirements, a secure VANET system should also support availability against various common attacks such as denial-of-service (DoS) attacks and replay attacks.

Most of the prior works on VANET security make exclusive use of public-key cryptography (PKC), requiring that every message be digitally signed and attached with public-key certificates. This incurs significant overhead in terms of both computational cost and bandwidth. In addition, signature verification is a much slower process than signature generation in proposed digital signature schemes, such as ECDSA, which makes it even more vulnerable to DoS attacks. Furthermore, the use of PKC may require infrastructure support (e.g. certificate revocation list distribution) which may not always be available everywhere even though VANET deployments are planned in the near future. Lack in full infrastructure deployment could be one of several reasons, such as insufficient funding or being offline due to a malfunction. The concerns mentioned above suggest that symmetric-key cryptography, which is overall much more efficient than public-key techniques, should be used so that VANET's real-time requirements can be met. However, it is infeasible to have every two vehicles share a secret session key due to the huge scale of VANETs. To address this problem, one solution is to use group communication which is motivated by the fact that in a VANET vehicles typically move in groups. The use of groups, together with symmetric-key cryptography can solve the key distribution problem and improve the efficiency of secure VANETs.

There are many VANET applications that require the formation of groups, particularly for vehicles in geographical proximity. The most prominent example is platooning, which groups vehicles in a way that allows them to accelerate or brake simultaneously, thereby avoiding collisions as well as increasing road capacity. VANET groups may also find numerous applications in infotainment in the future, such as multi-player games and chat rooms for vehicle passengers.

There are a number of ways to construct groups in VANET applications. The most useful category of groups in terms of functionality is a geodynamic group, where a group leader is elected dynamically, group membership is changed dynamically, and the group boundary also moves dynamically along the road with the vehicles in the group. Geodynamic groups are naturally the best choice for platooning-like applications.

Nonetheless, the design of secure VANETs is further complicated if groups are allowed to form, because security measures must be implemented to ensure only legitimate vehicles can join a group. In particular, the overhead associated with the formation and management of geodynamic groups poses a significant challenge in designing efficient security schemes (i.e. secure group communication). Herein, we propose a lightweight geodynamic group-based authentication protocol for VANETs which can efficiently create geodynamic groups and provide secure communication among the members of the groups via symmetric-key cryptography.

II. VANET SYSTEM

VANETs allow vehicles equipped with communication technology to perform efficient inter-vehicular communications (IVC) and road-vehicle communications (RVC) thereby enabling the Intelligent Transportation System (ITS) without the need for permanent infrastructure. Therefore, VANETs are also called inter-vehicle communication (IVC) or vehicle-to-vehicle (V2V) communications. Employing these networks will allow information about both surrounding traffic and road conditions to be relayed to the driver of the vehicle, thus allowing them to have an increased awareness of their surroundings.

Sensing applications could be incorporated to allow constant and real-time monitoring of the environment, surrounding roadways, or even monitoring of road conditions themselves. The recorded data could then be transmitted to the areas respective transportation authority for timely remediation if needed. A sample application depicting an accident and possible information exchange between various vehicles and roadside units (RSUs) is shown in Figure 1. For the rest of this, the terms "vehicle" and "node" will be used interchangeably.

The similarities of VANETs with other ad hoc networks such as Mobile Ad Hoc Networks (MANETs) are in their short radio transmission range, self- organization, self-management, and low bandwidth. However, VANETs can be distinguished from other kinds of ad hoc networks as follows: (1) highly dynamic topology due to high speed movement between nodes; (2) frequently disconnected network caused by high speed movement; (3) sufficient energy and storage provided by the vehicle; (4) geographical type of communication; (5) mobility modeling and prediction; (6) hard delay constraints such as in collision avoidance situation (e.g. Figure 1. Example of a safety application within a VANET the maximum delay of break event information will be very crucial); (7) and interaction with on-board sensors. Due to possibility of accidents, the exchange of information among vehicles is critical. This has put a lot of emphasis to security issues within VANETs. Security has started to receive a great deal of attention recently in addition to other issues regarding routing, medium access, connectivity, etc, As a VANET can be thought of as a specialized form of a MANET, several security challenges which are applicable to MANETs, apply to VANETs.

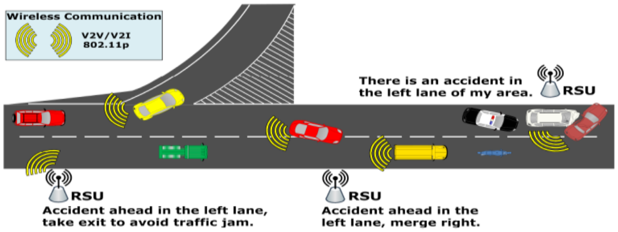
Wireless Communication
V2V/V2I
802.11p
There is an accident in the left lane of my area.
RSU
RSU
Accident ahead in the left lane, take exit to avoid traffic jam.
RSU
Accident ahead in the left lane, merge right.

Fig 1 Vanet System

VANETs go above and beyond MANET security challenges though; as nodes have identities which need to be protected but at the same time need to be identifiable should one misbehave. The increased mobility of nodes and the sheer size of the possible network are also unique security challenges.

Additionally, due to the initial intentions of a VANET being utilized to relay safety information between users driving, if the data is maliciously altered this could potentially cause fatalities. A detailed list of possible attacks, challenges, and discussion of proposed solutions can be found. To address the security issues in VANETs, the IEEE 1609 trial-use standard for Wireless Access in Vehicular Environments (WAVE) has been developed. The IEEE 1609.2 trial-use standard specifies security services for applications and communication management messages which are based on industry standards for public-key cryptography as will be explained in detail below.

A. IEEE 1609.2 FOR WAVE

The set of IEEE 1609 standards have been developed to enhance IEEE 802.11 standards for supporting wireless communication both between vehicles (V2V) and between vehicles and the roadside infrastructure (V2I). These are also commonly known as dedicated short range communications (DSRC) schemes. In particular IEEE 1609.2 addresses security within WAVE communications. The standard dictates that confidentiality, authenticity, and integrity must be provided within WAVE communications.

Though it identifies the usage of symmetric (secret-key), asymmetric (public-key), and hash functions as being able to provide these requirements, as far as authentication is concerned, IEEE 1609.2 identifies the utilization of public-key infrastructure (PKI) for establishing authenticity. As such, for authentication purposes, IEEE 1609.2 is based on public-key cryptographic standards, such as elliptic curve cryptography (ECC), as well as public standards for other PKI administration functions thereof, such as certificate revocation. Broadcast messages (e.g. safety vehicle warnings, vehicle safety messages) are defined as only being signed and, in general, not encrypted. As such, asymmetric techniques are again defined to be ideal. However, other transactional messages are left open to be protected by either symmetric or asymmetric means. The standard utilizes the SHA-1 hash function for creating identifiers for certificates and fragmented messages.

IEEE 1609.2 also defines an additional requirement of anonymity. That is the broadcast transmissions by a private individual should not reveal information which can be utilized in identifying them to unauthorized recipients. It is noted that vehicles, such as public safety vehicles, do not, in general, have an anonymity requirement. Though this extra requirement is identified, IEEE 1609.2, as dictated in [6], does not provide or define a mechanism for providing anonymity.

B. AUTHENTICATION IN VANETS

Authentication is a must feature in a VANET as the source of the information should be verified to ensure the legitimacy of the data communicated. We first identify a general attack model which is commonly utilized in VANET security analysis. Additionally, we provide several attack vectors based o_ of this threat model. Furthermore, we provide a discussion on the security goals and assumptions in designing an authentication scheme. The goals and assumptions presented reflect the majority of present work within VANET authentication research.

Attack Model

Although all possible attacks cannot be identified, several attack vectors that authentication schemes should attempt to protect against have been identified. Several authentication schemes reviewed herein utilized the following threat model detailed and summarized here. We utilized this threat model to guide us in decisions on what and how to protect while designing our protocol.
The general threat model is defined as follows:

Insider vs Outsider:

An insider is an authenticated node within the network and as such contains, at least, one valid key for usage with communicating with other nodes in the VANET. An outsider is a node which is not authenticated and as such is seen as a non-group member or intruder should they attempt to communicate within the group.

Malicious vs Rational:

A malicious attacker seeks to decrease network functionality or attack members of the network without the intent of personal gain. A rational attacker seeks personal gain from their attacks.

Active vs Passive:

Active attackers are capable of injecting messages into the network. Passive attackers only eavesdrop on communication going across the network.

Local vs Extended:

Local attackers control nodes or RSUs which are relatively close in location as a whole, thus limiting their view to a specific, localized area. Extended attackers control nodes or RSUs which are scattered throughout the network, thus giving them a broader, more generalized view of the network. Following in giving a generalized threat model, we also summarize several attack vectors. Most attacks defined in the reviewed papers directly stem from one or a combination of these attack vectors. As with the threat model, we utilized these attack vectors in guiding our design process for our protocol. Erroneous information propagation: Attackers attempt to propagate erroneous information throughout the network in an attempt to affect the actions taken by other nodes.

Cheating the sensors:

Attackers alter the readings of the sensors within the node (primarily their own sensors).

Identity disclosure:

The attacker is able to reveal the identity of the node and track their movements through network communications.

Denial of Service:

The attacker jams the channel or floods bogus messages in an attempt to overload the computation capabilities of nodes.

Masquerading:

Attackers attempt to assume the identity of another node or RSU.

Security Goals and Assumptions

Goals In addition to message authentication (which includes integrity), several of the reviewed schemes also identified other desirable goals sought within a VANET network based on their authentication model. Providing authentication may lead to exposing the location, driving pattern, and IDs of vehicles and drivers. Obviously, this is an important privacy concern for the drivers as exposing this information allows the driver to be tracked based solely on their message communication within the network, unbeknownst to them. In addition to privacy, another crucial goal is to meet the real-time constraints which are specific to VANETs. Any delay overhead introduced by an authentication process is not desirable as it may lead to fatalities. Though, as adding in various extra checks (e.g. authentication) will undoubtedly add additional delay, no matter how small, the impact to delay of any protocol should be kept down to a minimum. A non-exhausted list of security goals is given below:

Privacy (Anonymity):

Individual vehicles/drivers should be protected against unauthorized, identifying observations.

Real-time constraints:

Due to the high speed nature of a VANET, timely communications and strict time constraints should be enforced.

Availability:

The solution should not significantly increase or add in new attacks to deny communication ability (e.g., denial of service (DoS) from half-open connections).

Non-repudiation:

When needed, the identity of the sending vehicle should be recoverable from message communications, as well as ensuring the sender cannot deny transmitting the message.

Infrastructure Independency:

Due to possible unavailability of RSUs, a proposed solution should not require frequent access to an infrastructure when performing authentication.

Tamper Resistance

IEEE 1609.2 dictates that whenever practical, keying material should be protected from exposure and embedded in a tamper-resistant Hardware Security Module (HSM), also known as a tamper-proof device (TPD), on which many VANET authentication schemes also rely. A TPD is a physical device dedicated to secure storage of cryptographic keys and sensitive data as well as accelerating and securing cryptographic operations, with multiple layers of physical security measures that provide a high degree of tamper resistance. The primary goal of those devices is to make it difficult for an individual to access the material or data inside. It is accessible only by authorized personnel and it zeroizes its memory in the event of probing or scanning. We say difficult as most any device, given a sufficiently motivated/funded individual, could be eventually compromised.

A TPD:

- Houses the keying material
- Has a secure crypto processor
- Has its own battery
- Has its own clock (for timestamps)
- Has its own pseudorandom number generator for cryptographic operations
- Is accessible only by authorized personnel
- Zeroizes its memory in the event of probing or scanning

Without the assumption of at least a TPD, most VANET authentication schemes will be vulnerable to several attacks not previously noted as the keying material then becomes accessible by anyone. The primary drawback to a TPD, however, is that they can cost on the upwards of several thousand of dollars as of this writing. An alternative is the use of tamper resistance devices which can

provide security to a certain extent. These devices are cheaper compared to TPDs but the probability of being compromised is not 0%. Thus, the trade off in protocols for this becomes one of monetary cost versus data/user security.

C. C.CONNECTED DOMINATED SET

Nodes in wireless networks communication via a shared medium, either through a single hop or multi-hops. Such sharing reduces the network performance due to aggravated ratio interference. At same time it raises energy consumption since packet retransmission is needed when obstruction occurs. Moreover, the energy consumption could be increased if we don't limit number of active sensor nodes for the data relays. Backbone can be utilized to address the above evils. Backbone will remove unnecessary transmission links by end some of redundant nodes. Nevertheless backbone will still guarantee network connectivity in order to distribute data efficiently in a wireless ad hoc network. In virtual backboned based Wireless ad hoc network, some nodes are chosen as dominator node (backbone node) in the backbone structure process.

All nodes then can directly or indirectly converse with other nodes via these dominator nodes. The dominator form the backbone and the non-selected nodes can perform sleeping schedule or turn-off the ratio to save the energy consumption. Although, there is no physical backbone infrastructure, a virtual backbone can be formed by constructing a Connected Dominating Set (CDS). Given an undirected graph G = (V, E), a subset V' V))fV is a CDS of G if for each node u ε V, u is either in V' or there exist a node v ε V' such that uv ε E and the sub-graph induced by V', i.e., G(V'), is connected. The node in the CDS are called dominator or backbone node, other nodes are called dominate or non-backbone node. With the help of CDS, routing is easier and can adapt quickly to network topology changes. To reduce the traffic during communication and make simpler the connectivity management, it is desirable to construct a minimum CDS.

III. METHODS

In a VANET, communication often considers reporting specific events such as an emergency at a specific road position. Event based communication can be organized either according to the pull or the push communication paradigm [TvS02]. The consequences of applying these paradigms to

VANETs are evaluated in the following in order to determine which paradigm is more suitable for the majority of VANET applications.(a) pull-model (b) push-model.

The pull communication model is the traditional communication model in the Internet: An application sends a request, the request is forwarded to a node at the destination, and the destination node sends a reply including the requested Information.

In contrast, the push communication model is based on the idea that nodes sensing events of interest continuously "push" the information into the network. For example, a vehicle detecting a traffic jam situation would disseminate this information via the VANET. The information would be forwarded (not necessarily unchanged, e.g. it could be forwarded in an aggregated form) to all vehicles in the local area.

Data dissemination schemes for VANETs that have been proposed in literature can be grouped in the following two categories:

1. Using an (adapted) ad hoc routing mechanism to establish a point-to-point connection from one vehicle to another,

2. Flooding the local area (limited by the number of hops or by geocast) of the vehicle.

Routing approaches are typically used by applications applying the pull communication model, since these applications require a route from source to destination. In contrast, push communication can best be implemented based on flooding or broadcast schemes.

Acknowledged Broadcast from Static to highly Mobile (ABSM) protocol. Broadcasting is a task of sending message to all the nodes in the network. It is also referred as Data Dissemination. The main objective of Vehicular communication is to create a efficient and reliable protocol to broadcast the message in the network. The DV-Cast protocol deals with various connectivity conditions but it works only for straight roads. It does not support interconnection roads. PBSM protocol is similar to ABSM protocol but it does not handle redundant transmissions. To overcome these problems ABSM provides solution, it gets the position information through beacon messages and with this information it forms CDS network and broadcast messages. It maintains R and N list, and timeout. It updates these three during every packet transmission. By maintaining R and N list it avoids retransmission. Since CDS network is used here, this protocol supports for intersection roads. Here the nodes which are in CDS set only transmit the packets. So it avoids redundant transmissions. Hence it saves energy.

IV. THE PRBP PROTOCOL

It is an adaptive broadcasting protocol that does not require nodes to know about position and movement of their nodes and itself. It uses connected dominating sets (CDS) and neighbor elimination concepts to eliminate redundant broadcasting. It employs two-hop neighbor information obtained by periodic beacons to construct CDS. Each vehicle A maintains two lists of neighboring vehicles: R and NR, containing neighbors that already received and that which did not receive the packet. After a timeout, A rebroadcasts the packet if the list.NR is nonempty. Both lists R and NR are updated periodically by using beacon messages. Nodes in CDS have less waiting timeout than nodes that are not in CDS. The main idea of PBSM is two nodes do not transmit every time they discover each other as new neighbors. PGB is not a reliable broadcasting protocol but it is a solution to prevent broadcast storm problem from route request broadcasting. Each node in PGB will sense the level of signal strength from neighbor broadcasting. The signal strength is used for waiting timeout calculation. Nodes in the edge of circulated broadcast will set shorter waiting timeout.

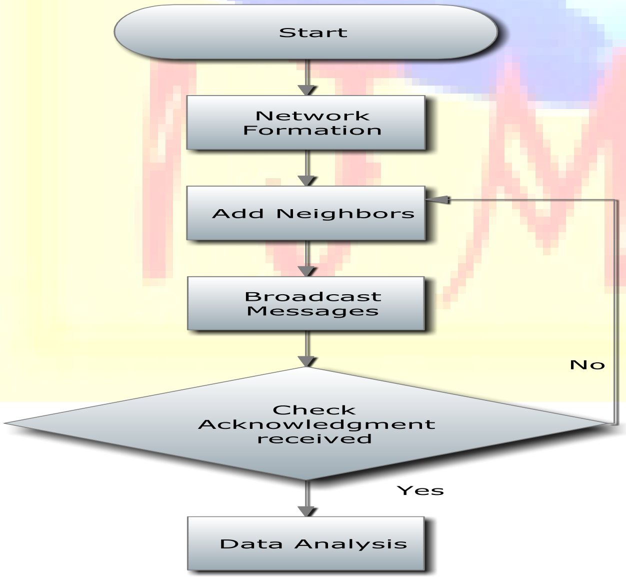

Fig 2 Flow chart diagram for PRBP protocol

V. KEY GENERATION

key is generated to provide security during the transmission. For key generation RSA algorithm is used.

RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated the following way:

Choose two distinct prime numbers p and q.

For security purposes, the integer's p and q should be chosen uniformly at random and should be of similar bit-length. Prime integers can be efficiently found using a primarily test. Compute n = pq. n is used as the modulus for both the public and private keys. Compute φ(pq) = (p − 1)(q − 1). (φ is Euler's totient function). Choose an integer e such that 1 < e < φ(pq), and e and φ(pq) share no divisors other than 1 (i.e., e and φ(pq) are coprime). e is released as the public key exponent. e having a short bit-length and small Hamming weight results in more efficient Encryption. However, small values of e (such as e = 3) have been shown to be less secure in some settings. Determine d (using modular arithmetic) which satisfies the congruence relation d e \equiv 1\pmod{\varphi(pq)}.Stated differently, ed − 1 can be evenly divided by the totient (p − 1)(q − 1). This is often computed using the extended Euclidean algorithm. d is kept as the private key exponent.

VI. RESULT

We have simulated the proposed model along with the previously used model. The proposed shows that the more no of packet transmission. Some results for the most disconnected scenario (75 sec between injected vehicles per route) are shown in We focus on this scenario because reliability results improve in general as the interval between injected vehicles decreases, since it means a more connected network. Therefore, all protocols, for each model, tend to achieve 100 percent reliability.

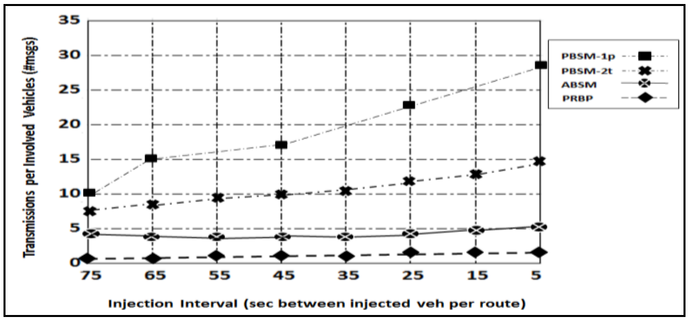

Fig 4 Number of data transmissions per involved vehicle.

Number of data transmissions per involved vehicle is simulated in the graph. PRBP protocol has high reliability in data dissemination.

VII. Conclusion

PRBP Position aware reliable broadcasting protocol improves the efficiency and reliability of the network. Each vehicle in the network collects the position of the neighbors from the beacons passed in network. Based on the position information it selects the neighbor nodes in preferred distance to broadcast the messages. The selected nodes will broadcast the messages to all the victims in the network.

In case of failure of selected nodes, the transmission of those messages will take care by closest node of selected node. Based on the timing of received messages waiting timeout is calculated and messages will broadcast through them. The acknowledgment of each node is piggyback to the beacon. So the other nodes can identify whether their neighbors will received or not. Because of piggyback acknowledgments and transmission by neighbor nodes during failure cases it provides efficient and reliable transaction.

VIII. REFERENCES

[1] Wu. L, and Li. H “A Dominating Set Based Routing Scheme in Adhoc Wireless Networks” Telecomm. Systems, Vol. 18,nos. 1/2, PHP, 2002.

[2] Viswanath.K and Obraczka.K, “An Adaptive Approach to Group Communications in Multihop Ad Hoc Networks,” Proc. IEEE Int’l Symp. Computers and Comm. (ISCC’02), pp.559-566, 2002.

[3] Stojmenovic.I and Wu.J, “Broadcasting and Activity Scheduling in Ad Hoc Networks,” Mobile Ad H Networking, Basagni. S, Conti. M, Giordano. S and Stojmenovic. I, eds., pp.205-229, IEEE Press, 2004.

[4] Korkmaz.G, Ekici.E, Ozguner. G, and Ozguner. U, “Urban Multi-Hop Broadcast Protocol for Inter-Vehicle Communication Systems,”Proc. First ACM Int’l Workshop Vehicular Ad Hoc Networks(VANET ’04), pp. 76-85, Oct. 2004.

[5] Lee.U, Lee.J, Park.J, Amir.J, and Gerla.M, “FleaNet: A Virtual Market Place on Vehicular Networks,” Proc. Third Ann. Int’l Conf. Mobile and Ubiquitous Systems: Networking and Services, pp. 1-8, July 2006.

[6] Biswas.S, Tatchikou.T, and Dion.F, “Vehicle-to-Vehicle Wireless Communication Protocols for Enhancing Highway Traffic Safety,” IEEE Comm. Magazine, vol. 44, no. 1, pp. 74-82, Jan. 2006.

[7] Korkmaz.G, Ekici. E, and Ozguner.F, “An Efficient Fully Ad-hocMulti-Hop Broadcast Protocol for Inter-Vehicular Communication Systems,” Proc. IEEE Int’l Conf. Comm. (ICC ’06), June 2006.

[8] Khan.A, Stojmenovic.I, and Zaguia.N, “Parameterless Broadcasting in static to Highly Mobile Wireless Ad hoc, Sensor and Actuator Networking and Applications(AINA’08) Mar. 2008

[9] Ros. F, Ekici. E, and Ozguner. F, “An Efficient Fully Ad Hoc Multi Hop Broadcast in Vehicular Ad Hoc Networks,” Proc. 69th IEEE Vehicular Technology Conf. (VTC ’09) Apr. 2009.

[10] Li.M, Lou.W, and Zeng.K, “OppCast: Opportunistic Broadcast of Warninf Message in VANETs with Unreliable Links”, Proc. IEEE Sixth Int’l Conf. Mobile Ad hoc and Sensor Systems (MASS’09), Oct 2009.

[11] M. Torrent-Moreno, D. Jiang, and H. Hartenstein, “Broadcast Reception Rates and Effects of Priority Access in 802.11-Based Vehicular Ad-Hoc Networks,” Proc. First ACM Int’l Workshop Vehicular Ad Hoc Networks (VANET ’04), pp. 10-18, Oct. 2004.

[12] V. Taliwal, D. Jiang, H. Mangold, C. Chen, and R. Sengupta, “Empirical Determination of Channel Characteristics for DSRC Vehicle-to-Vehicle Communication,” Proc. First ACM Int’l Work-shop Vehicular Ad Hoc Networks (VANET ’04), pp. 88-88, Oct. 2004