Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 11, November 2014, pg.713 – 723

RESEARCH ARTICLE

A NOVEL CROSS LAYER PRIVACY PRESERVING IN VEHICULAR AD-HOC NETWORK

Mrs. R.Logapriya[1], Mrs. R.Kavitha[2]

[1]M.Phil Research Scholar Department of computer science Vivekanandha College for Women

[2]Assistant Professor Department of computer science Vivekanandha College for Women, Tiruchengode, Namakkal

[1] logapriya4891@gmail.com, [2] kavithamscmphil@gmail.com

ABSTRACT- The traffic data collection mechanisms have relied on fixed sensor networks, including inductive loop detectors, wireless magnetometer sensors, and microwave radar sensors. Because these dedicated sensing systems are expensive to install and maintain, their deployment has been limited largely to highways. As a result, traffic information on many of the major arterial roads is sorely lacking. At present a vehicular for the city road scenario with an assumption that each safety message carries the location information of the sending vehicle. Verifiers of each message are defined according to their locations in relation to the sender. Only the selected verifiers check the validity of the message while non-verifiers of the message rely on verification results from these verifiers. A brand new research issue of the VPKI is how to select verifiers in the city road scenario. For security purpose the RSA three key generation techniques. The authentication is a key barrier in the network information system security field. RSA is an open network environment technology, using public key cryptogram system theory has implemented and supplied a universal security infrastructure for security services, it has two main applications, include encryption and digital signature.

NOVEL TRAFFIC MONITORING SYSTEM

Introduction

Proposed a novel traffic monitoring system design based on the concept of virtual trip lines (VTLs) and experimentally evaluate its feasibility. Virtual trip lines are geographic markers stored in the mobile phone client, which trigger a position and speed update when a probe vehicle trajectory intersects a trip line. Through privacy-aware placement of these trip lines, clients need not rely on a trustworthy server. The system is designed for GPS-enabled cell phones to enable rapid software deployment to a large and increasing number of programmable smart phones.

Here present a cooperative message authentication protocol (VPKI) for the city road scenario with an assumption that each safety message carries the location information of the sending vehicle. Verifiers of each message are defined according to their locations in relation to the sender. Only the selected verifiers check the validity of the message while non-verifiers of the message rely on verification results from these verifiers.

The security purpose it provide triple key generation techniques. The authentication is a key barrier in the network information system security field. That Crypto technique is an open network environment technology, using public key cryptogram system theory has implemented and supplied a universal security infrastructure for security services, it has two main applications, include encryption and digital signature. Along with the modern times autoimmunization improvements, a great deal of no face-to-face electronic trades are increasing. A veracity, and security, and practicable automatic personal identification are even more highly demanded and required in our life.

Traffic monitoring using GPS-equipped vehicles raises significant privacy concerns, because the external traffic monitoring entity acquires fine-grained movement traces of the probe vehicle drivers. These location traces might reveal sensitive places that drivers have visited, from which, for example, medical conditions, political affiliations, traffic violations, or potential involvement in traffic accidents could be inferred. Traffic monitoring does not need to rely on individuals or personal information, only on the aggregated statistics from a large number of probe vehicles.

VIRTUAL TRIP LINE CONCEPT

The traffic monitoring system builds on the novel concept of virtual trip lines and the notion of separating the communication and traffic monitoring responsibilities. A virtual trip line (VTL) is a line in geographic space that, when crossed, triggers a client's location update to the traffic monitoring server.

More specifically, it is defined by [id; x1; y 1; x2; y 2; d]:

Where id, is the trip line ID, x1, y1, x2, and y2 are the (x; y) coordinates of two line endpoints, and d is a default direction vector(e.g., N-S or E-W). When a vehicle traverses the trip line its location update comprises time, trip line ID, speed, and the direction of crossing. The trip lines are regenerated and stored in clients. To check any crossings, here set the sampling period of a single-chip GPS/A-GPS module in each Smartphone and retrieve the position readings.

Virtual trip lines control disclosure of location updates by sampling in space rather than sampling in time, since clients generate updates at predefined geographic locations, compared to sending updates at periodic time intervals. Through careful placement of trip lines the system can thus better manage data quality and privacy than through a uniform sampling interval. In addition, the ability to store trip lines on the clients can reduce the dependency on trustworthy infrastructure for coordination.

TRAFFIC MONITORING WITH VIRTUAL TRIP LINES

Here introduce the concept of virtual trip lines for privacy-preserving monitoring and describe two architectures that embody it. The first architecture seeks to provide probabilistic privacy guarantees with virtual trip lines.

Design Goals

To achieve both high quality traffic information and strong privacy protection in this traffic monitoring system. There exists an inherent tradeoff between these requirements, since privacy-enhancing technologies such as spatial cloaking reduce accuracy of traffic monitoring.

Privacy

The privacy protection by design so that the compromise of a single entity, even by an insider at the service provider, does not allow identifying or tracking users. Data Integrity. The system should not allow adversaries to insert spoofed data, which would reduce the data quality of traffic information. This is especially challenging because it conflicts with the desire for anonymity.

Smartphone Client

The client software must cope with the resource constraints of current smart phone platforms. One may expect, however, that a privacy-preserving design motivates more users to participate in such a system, which would improve the quality of traffic information.

NETWORK FORMATION

Here, used ns2 simulator on Linux machine. Because, it focuses on the link stability and route lifetime, no route overhead was considered in our simulation. In 3000 X 500 m^2 area, mobile nodes exist. Here used square area to increase average hop length of a route with relatively small nodes. Every mobile node is moving based on mobility data files that were generated by mobility generator module. The transmission range is fixed at 250 units. 20 nodes of them have destinations and try finding routes to their destination nodes.

ELLIPTICAL CURVE CRYPTOGRAPHY ALGORITHM

Packet forwarding

It capture the transfer message packet from nodes which wand to send the data and it retrieve the packet source and destination address. After gathering the both address it take this next hop address from that packet then it check this next hop address to its network neighbor list which has high performance from existing evaluation. If this next hop is present in the neighbor list it simple transfer packet to next hop otherwise it simple delete the packet from its network.

Elliptical curve cryptography

Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible - this is the "elliptic curve discrete logarithm problem" or ECDLP. The entire security of ECC depends on the ability to compute a point multiplication and the inability to compute the multiplicand given the original and product points. The size of the elliptic curve determines the difficulty of the problem.

The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements, i.e. that an elliptic curve group could provide the same level of

security afforded by an RSA-based system with a large modulus and correspondingly larger key—e.g., a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public key For current cryptographic purposes, an *elliptic curve* is a plane curve which consists of the points satisfying the equation

$$y^2 = x^3 + ax + b,$$

Key Generation

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key. Now, it have to select a number's' d within the range of 'n'. Using the following equation we can generate the public key

$$Q = d * P$$

'Q' is the public key and 'd' is the private key. 'd' is the random number that it have selected within the range of (1 to n-1). P is the point on the curve.

Let 'm' be the message are sending. It have to represent this message on the curve. These have in-depth implementation details. All the advance research on ECC is done by a company called certicom. Consider *'m'* has the point *'M'* on the curve *'E'.* Randomly select 'k' from [1 - (n-1)]. Two cipher texts will be generated let it be **C1** and **C2.**

$$C1 = k*P$$

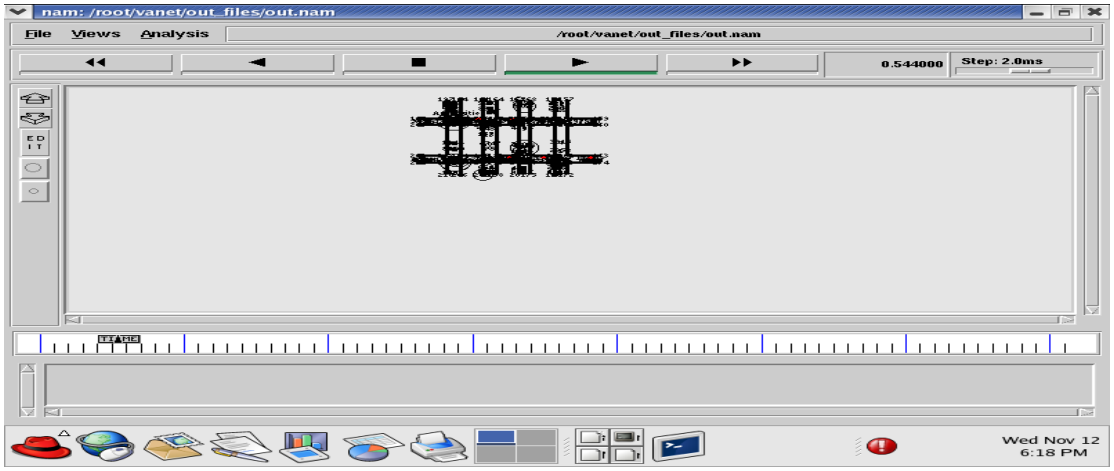
$$C2 = M + k*Q$$

$$M = C2 – d * C1$$

It have to get back the message 'm' that was send to us, M is the original message that it have send.

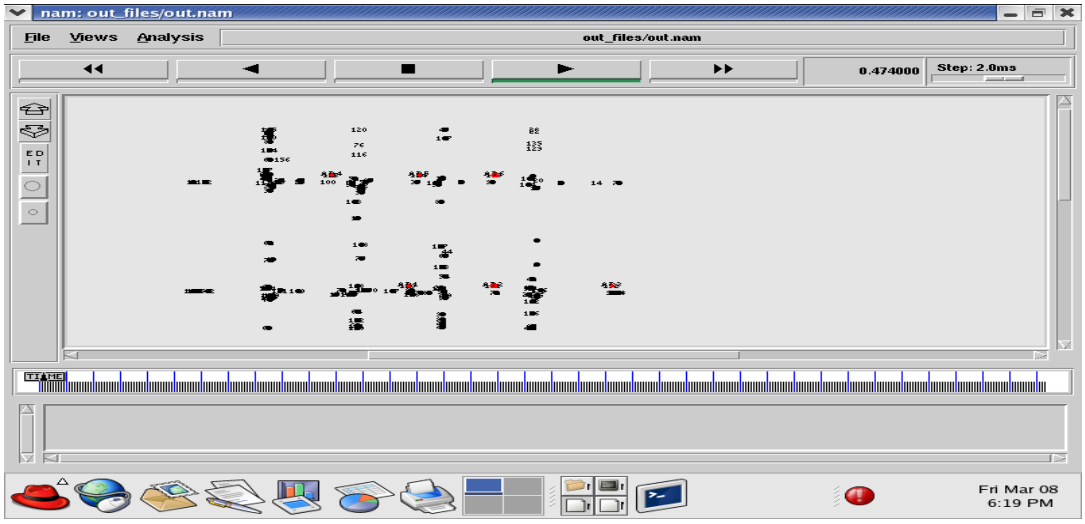
EXPERIMENT AND RESULTS

Network Formed



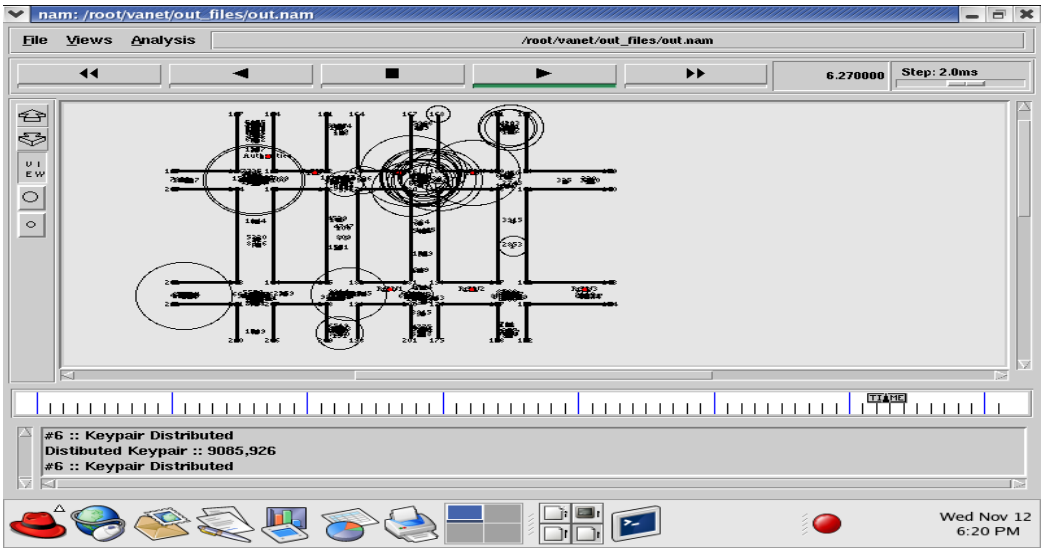
Experimental results shows that the networks formed and road side units are created for vehicular network. Road side edges and borders are initiated and it is specified in the following simulation results as shown above.

Node Communication



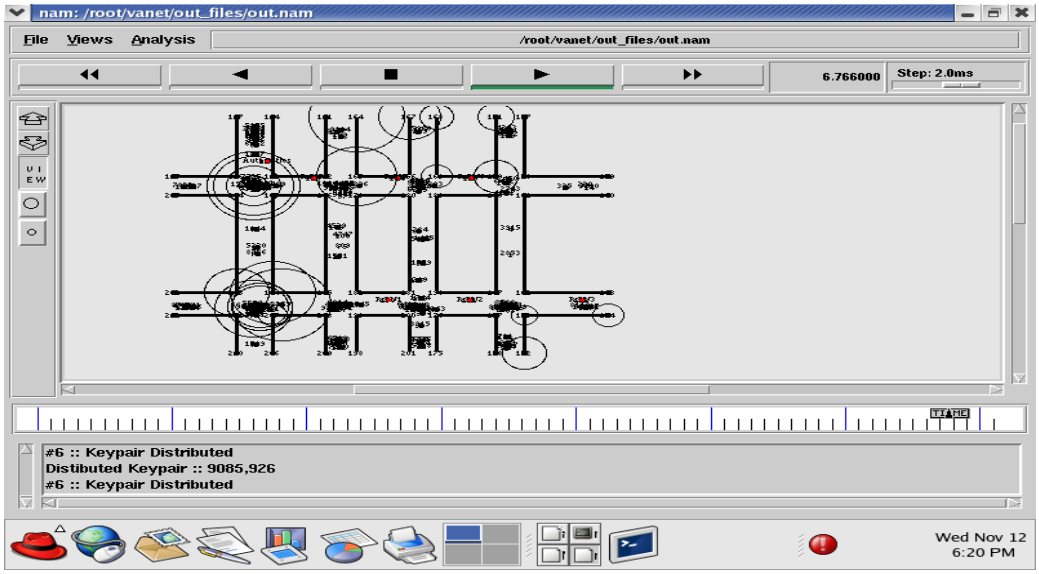
Secured & Privacy preserving scheme is implemented in routing is established and the nodes are communicated.

Node Authentication



The above graph shows that the Nodes are getting authentication from the agent node for vehicles flow direction**.**

Secured File Transmission



The above graph shows that the secured file transmission has to implemented and pairing keys are distributed and after authentication if it is successful then it will be communicated successfully

Number Of Attacker Node Vs Average Dropped Packet

The Existing System, where number of attacker nodes increases because of that the number of packet dropped also increase. In proposed system, when No of attacker increases which leads to reduces number of packets drop. Hence, proposed system provides strong security than the existing one.

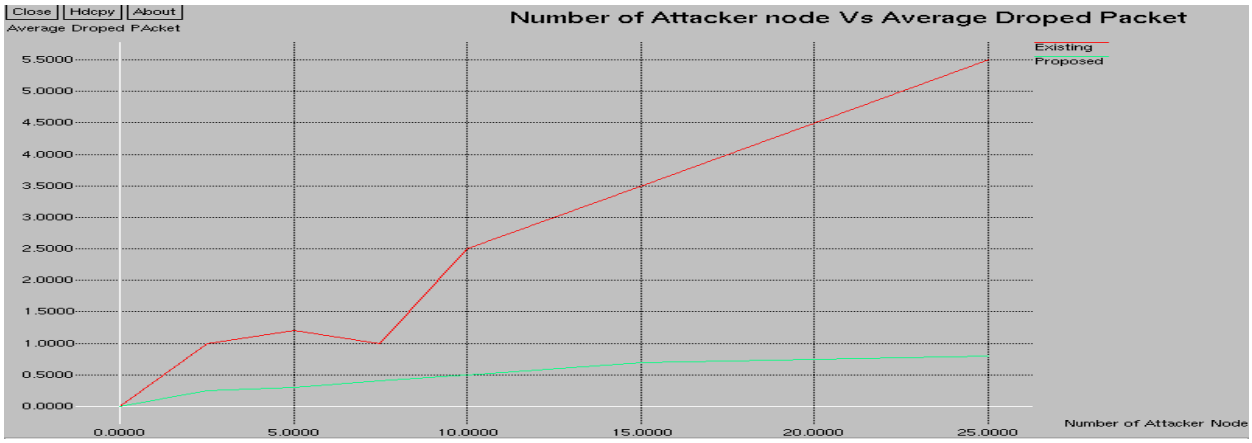


Fig.1 Number of attacker node Vs Average Dropped packet

Number Of Nodes Vs Average Latency

Latency means the amount of time a message takes to traverse a system. In a computer network, it is an expression of how much time it takes for a packet of data to get from one designated point to another. It is sometimes measured as the time required for a packet to be returned to its sender. Hence, proposed system is highly efficient than the existing one.

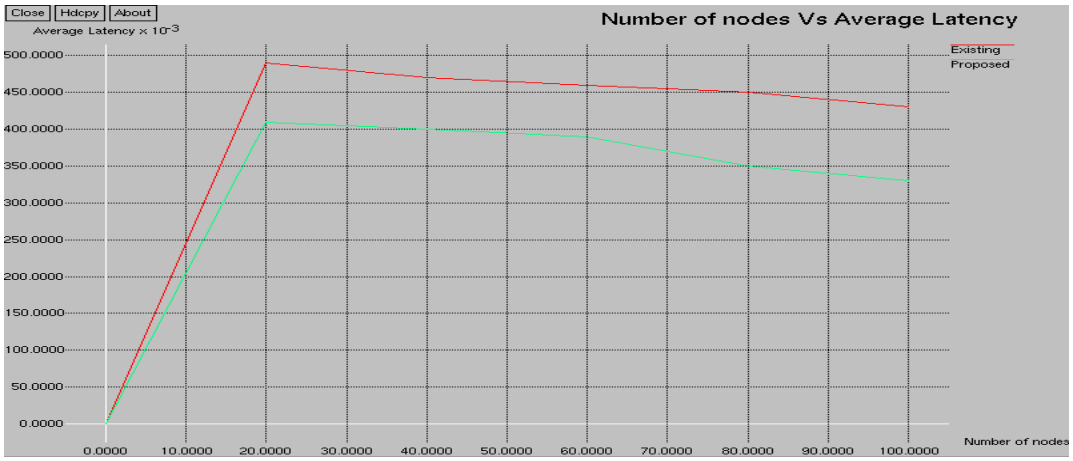


Fig.2 Number of nodes Vs Average Latency

Number Of Attacker Nodes Vs Average Overhead

This graph shows that No of Attacker nodes Vs Average overhead compared with the existing and proposed system. From the below graph, shows that in the existing system when number of attacker nodes increase the average overhead also increase. To overcome the existing problem of increasing overhead we implement our proposed system to reduce the overhead when number of attacker node.

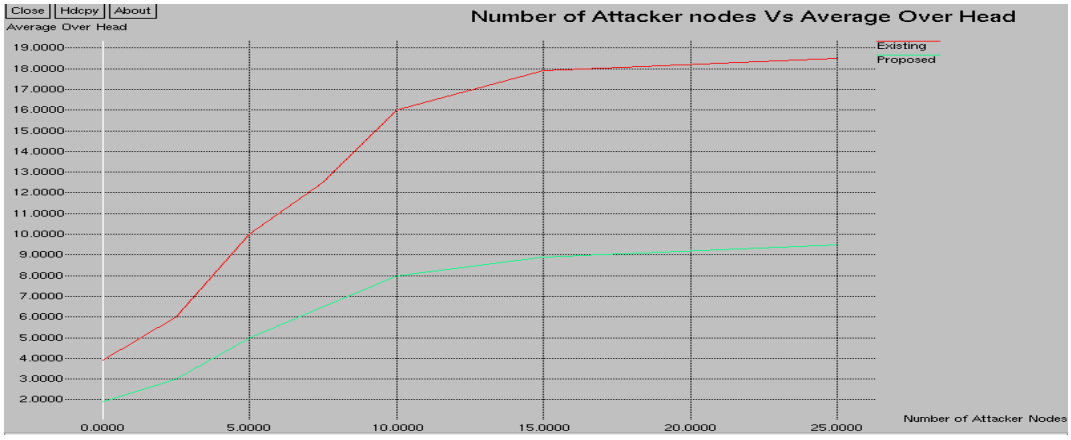


Fig.3 Number of attacker nodes Vs Average over head

No Of Nodes Vs Packet Delivery Ratio

This graph shows that No of nodes Vs packet delivery ratio compared with the existing and proposed system. From the above graph, it represent proposed System is high in packet delivery ratio when compare to the existing system**.**

Packet delivery ratio: the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

$\sum$ Number of packet receive / $\sum$ Number of packet send.

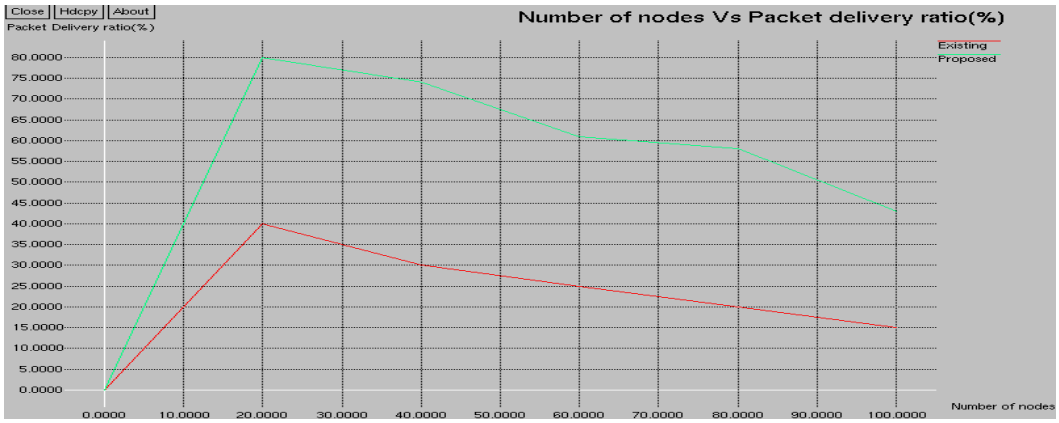


Fig.4 Number of nodes Vs Packet delivery ratio

CONCLUSION AND FUTURE ENHANCEMENT

The traffic information on many of the major arterial roads is sorely lacking. A comparison of the efficiencies of three key-management schemes for a VANET has been performed. From the results it has been shown that there is an increase in the efficiency of the system when there is a scheme in place. There is a considerable improvement in the data communication between the nodes after key management techniques have been employed. Out of the three schemes, it is found that the RSA algorithm is found to be the most efficient out of the other algorithm model used in existing. All this has been proved on by simulation on the Network Simulator 2 tool .At critical security areas which are prone to attacks a key management technique is absolutely compulsory. Without it the delivery ratio becomes so less that there is no meaningful data communication possible. This technique can be used in security-sensitive applications like police and government agencies where VANETs are increasingly being used.

Cost effectiveness of the system: It should be said that implementing our proposed system will lead to many solutions of the security problems that are encountered in VANET. Even the system is costly. So an imperative solution of this system and an effective cost management analysis of this system can be a great future research issue. Time delay management: VANET is an excellent discovery in terms of safety related information. If the information send later, i.e. after a good amount of time then it will be useless to have such a system. So reducing time delay should be a prime research topic.

REFERENCES

[1] O. Andrisano, et. al, Intelligent transportation systems: The role of Third-Generation mobile radio networks, IEEE Communications Magazine , 38(9):144-151, 2000.

[2] Standard Specification for Telecommunications and Information Exchange Roadside and Vehicle Systems- 5GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications, ASTM International, April 2009.

[3] IEEE 802.11 Working Group, Part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications, ANSI/IEEE Std. 802.11, Sept. 1999.

[4] F. Qu, F. Wang, L. Yang, Intelligent transportation spaces: vehicles, traffic, communications, and beyond, IEEE Communication Magazine, 48(11): 136-142, 2010.

[5] Report: Overview of the C2C-CC System, CAR 2 CAR Communication Consortium, August, 2007.

[6] M. T. Moreno D. Jiang, H. Hartenstein, Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks, ACM Int. Workshop on Vehicular Ad Hoc Networks (VANET'04), pp. 10-18, 2004.

[7] Q. Xu, T. Mak, J. Ko, and R. Sengupta, Vehicle-to-vehicle safety messaging in DSRC, ACM VANET, pp. 19-28, 2004.

[8] X. Ma, X. Chen, and H. Refai, On the broadcast packet reception rates in one-dimensional MANETs, IEEE GLOBECOM 08, Nov. 30-Dec. 4, New Orleans, 2008.

[9] N. An, T. Gaugel, and H. Hartenstein, VANET: is 95% probability of packet reception safe? IEEE 11th International Conference on ITS Telecommunications, 2011.

