International Journal of Engineering Research and General Science Volume 4, Issue 4, July-August, 2016
ISSN 2091-2730

Secure Data Transmission Using Improved Diffie-Hellman Algorithm in VANET

[1]Dr. T.Ramaprabha, [2]V.Premalatha

[1]Professor, Department of Computer Science and Applications,

[2]Full Time M.Phil Scholar, Department of Computer Science,

[1,2]Vivekanandha College of Arts and Science for Women,Tiruchengode, Tamilnadu, India.

[1]ramaradha1971@gmail.com , [2]premkani11@gmail.com

Abstract- A Vehicular Ad-Hoc Network is a form of mobile ad hoc network, which provide communications among nearby vehicles and nearest fixed equipment, like traffic sensor. Vehicular network act as an infrastructure to transfer the data between vehicles. Road Side Unit acts as a base station to deliver the data about the path to the vehicles using Diffie-Hellman key exchange algorithm. It is one of the more popular and interesting methods of key distribution. It is a public-key cryptographic system whose sole purpose is for distributing secured keys and avoiding activities of attackers.It gives high level security and more energy efficient data transmission on the network. Diffie-Hellman key exchange is used to find out another route quickly in the case of false route. It also used to recover the failure nodes. In this paper, we discuss about the secure data transmission using Improved Diffie – Hellman algorithm in VANET.

Keywords- VANET, Security, Privacy, RSU, OBU

INTRODUCTION ON VANET

The Vehicular Ad-Hoc Network, or VANET, is a technology that uses moves cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 metres of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that mobile internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes.

Vehicular network faces wide range of attacks and the most common attacks are: impersonation, bogus information injection, non integrity, non confidentiality, and Denial of Service (DOS). Two classes of attacks are like to occur in vehicular networks such as

1. external attacks, in which attackers not belonging to the network jam the communication or inject erroneous information.

2. Internal attacks, in which attackers are internal compromised nodes that are difficult to be detected.

Both types of attacks may be either passive intending to steal information and to eavesdrop on the communication within the network, or active modifying and injecting packets to the network. As a counter-measure against most of these attacks, the following security considerations should be satisfied providing a trusted infrastructure between communicating vehicles, mutual authentication between each communicating pair whether two vehicles or a vehicle and a fixed element of infrastructure, efficient access control mechanisms allowing not only the authorization to the network access but also the authorization to the services' access, confidential and secure data transfer.

Since ITS (Information Technology scheme) applications are mainly targeting the peoples' safety on roads, while passengers oriented Non-ITS applications are mostly concerned with commercial services provision on roads, thus Securing inter vehicular communication is different in both cases as shown in figure 1.1. As a consequence security requirements are different for each application type.

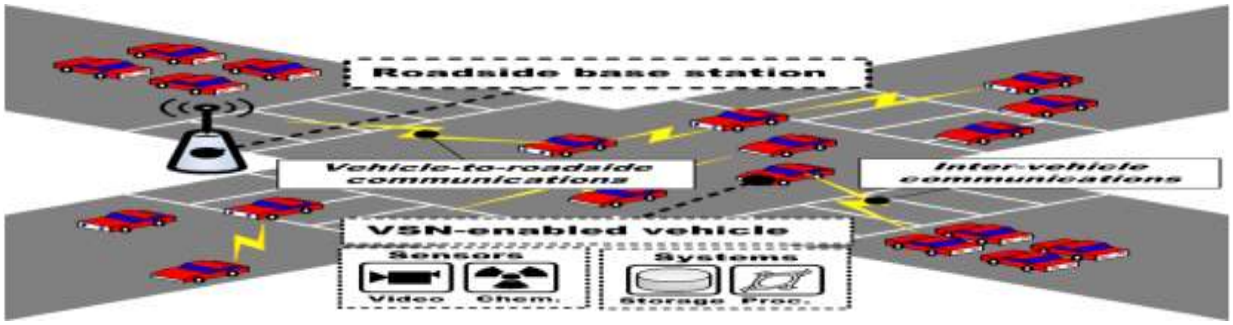

Figure 1.1: Communication Based on Vehicular Network by using the RSU

For both types of applications, we found that the non-repudiation, the integrity and the non-traceability is important security requirements for worth considerations. Thus a complex problem arises in this issue.

In fact, a tough requirement in vehicular networks environments is to manage traceability in terms of allowing this process for the concerned authorities and at the same time assuring the no traceability between mobile client's vehicles themselves. Nevertheless, the latter is difficult to be achieved and so far no promising solutions exist to resolve this issue in the vehicular networks dynamic and open environment. It is noticed that the word traceability can include:

1. Authentication, Authorization and Access Control.
2. Vehicular applications and Internet Implementations.
3. Routable addresses and position based addressing.

NEED OF SECURE DATA TRANSMISSION

Since the authentication scheme is susceptible to malicious attacks, the objective is to design a scheme that is robust to such attacks. Based on related studies. the following key security requirements for VANETs is defined.

1. **Efficiency:** In VANETs, the computational cost of vehicles must be as low as possible in order to have a real-time response.

2. **Anonymity:** The anonymous authentication procedure verifies that an OBU does not use its real identity to execute the authentication procedure.

3. **Location privacy:** An adversary collects the serial authentication messages of the OBU but it still failed to track the location of the vehicle.

4. **Mutual authentication:** A mutual authentication procedure is implemented whereby the LE must verify that the OBU is a legal user and the OBU must ensure that the LE is genuine.

5. **Integrity:** The message integrity means that data cannot be modified undetectably.

Vehicular networks permit [3] cars to communicate with each other and with a distinct infrastructure on the road. Infrastructures can be purely ad hoc between cars or facilitated by making use of an infrastructure. The organization typically consists of a set of so called roadside units that are connected to each other or even to the Internet [1].
VANET uses three systems:

1. Intelligent transportation systems
2. Vehicle-to-roadside communication and
3. Routing-based communication.

Intelligent Transportation Systems: The inter-vehicle communication conformation uses multi-hop multicast or programme to transmit traffic correlated information over multiple hops to a group of receivers. In intellectual transportation systems, vehicles need only be concerned with activity on the road forward and not behind.

Vehicle-to-Roadside Communication: The vehicle-to-roadside communication formation characterizes a single hop transmission where the roadside unit sends a broadcast message to all prepared vehicles in the vicinity. Vehicle-to-roadside communication formation provides a high bandwidth link between automobiles and roadside units. The roadside units may be placed every kilometre or less, succeeding high data rates to be continued in heavy traffic [2].

Routing-Based Communication: The routing based communication arrangement is a multi-hop unicast where a message is broadcasted in a multi Routing based announcement hop fashion until the vehicle carrying the anticipated data is reached. When the request is received by a vehicle preserving the desired piece of information, the application at that vehicle instantly sends a unicast message containing the information to the vehicle it established the request from, which is then exciting with the task of forwarding it towards the query source.

DIFFIE-HELLMAN KEY EXCHANGE ALGORITHM

It should be complemented with an authentication mechanism. In this approach for key distribution with security factors to solve attacking problem is very challenging and that the shared key is never itself transmitted over the channel. A distributed key management framework has advantage in revocation of malicious vehicles, system maintenance, and the implementation of heterogeneous security policies. The basic Structure of Diffie-Hellman Algorithm figure 3.1 as shown in below.

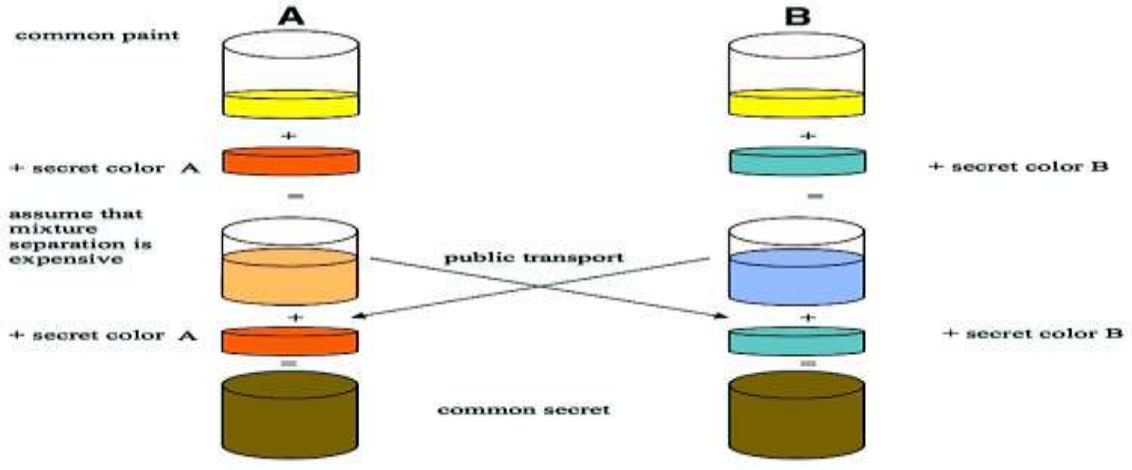

Figure 3.1 Structure of Diffie-Hellman Algorithm

A secure key distribution protocol is used with the capability of preventing from misbehaving. The protocol guarantees the traceability of compromised malicious vehicles.An efficient cooperative message authentication protocol is developed, by which cooperative verifiers are intelligently selected to significantly reduce the computation and communication overhead in the group signature based implementation.

A. Key Generating Node

Active attackers have the ability to send packets into wireless channels. Global attackers have an unlimited scope which means they can listen to any information in the network. Attackers May have strong transmission power to communicate over long distances. Adversarial parsimony means an attack involving a few malicious nodes is more likely to happen than an attack that requires collusion among a large number of nodes. The key generating node(KGN) will assume that the vehicles will report to authorities when they find that the other vehicle sends a false message. Wired network which connects authorities transmits data securely without packet loss. In the key distribution phase, our protocol is used to moderator whether a vehicle is a legitimate user or not.

B. Road Side Unit (RSU)

The RSU [4] Detection System using the Diffie Hellman key exchange method used to be one of the most interesting key distribution schemes in use today. However, one must be aware of the fact that although the algorithm is safe against passive dropping, it is not necessarily protected from active attacks distribution to allow malicious nodes to interact within the network for transferring data between sources to destination and hence complete security could not be achieved within the network due to the

presence of malicious nodes. In order to provide more secure communication between source and destination, DH uses risk as an input to determine how much source node can be trusted, so that only trusted nodes are allowed to communicate and hence high security can be achieved within VANET. They have to take a throughput, delay and delivery ratio are network performance on the network. It most efficient and security based data transmission.

Advantages

- Diffie-Hellman algorithm is used to find out another route easily.
- Each user have own time slot.
- Efficient data transformation.
- Data will be transferred without any packet loss.
- Network performance is increased effectively.

DIFFIE-HELLMAN ALGORITHM IMPLEMENTATION IN NS-2

Ns or the Network simulator (also popularly called ns-2) is a discrete event network simulator. It is popular in academia for its extensibility (due to its open source model) and plentiful online documentation. Ns are popularly used in the simulation of routing and multicast protocols among others and are heavily used in ad-hoc networking research. Ns supports an array of popular network protocols, offering simulation results for wired and wireless networks alike. It can be also used as limited –functionality network emulator. Ns are licensed for use under version 2 of the GNU General Public License.

A. Network Simulator 2.28 (NS-2)

Ns-2.28 is a packet-level simulator and essentially a centric discrete event scheduler to schedule the events such as packet and timer expiration. Centric event scheduler cannot accurately emulate “events handled at the same time” in real world, that is, events are handled one by one. This is not a serious problem in most network simulations, because the events here are often transitory. Beyond the event scheduler, ns-2 implements a variety of network components and protocols. Notably, the wireless extension, derived from CMU Monarch Project, has 2 assumptions simplifying the physical world. Nodes do not move significantly over the length of time they transmit or receive a packet. This assumption holds only for mobile nodes of high-rate and low-speed. Consider a node with the sending rate of 10Kbps and moving speed of 10m/s, during its receiving a packet of 1500B, the node moves 12m. Thus, the surrounding can change significantly and cause reception failure. Node velocity is insignificant compared to the speed of light.

B. Simulator Setup NS-2

NS-2 is an open-source simulation tool running on Unix-like operating systems. It is a discreet event simulator targeted at networking research and provides substantial support for simulation of routing,multicast protocols and IP protocols, such as UDP, TCP, RTP and SRM over wired, wireless and satellite networks. It has many advantages that make it a useful tool. LAN routing and broadcasts are part of routing algorithms.TCL script is used for configuring and parameterizing a simulation. Using Diffie-Hellman algorithm we implemented the NS-2 simulator to improve the performance of secure data transmission in VANET as shown in below figures.

This module figure 4.1 is developed to node creation and more than 10 nodes placed particular distance. wireless node placed intermediate area. Each node knows its location relative to the sink. The access point has to receive transmit packets then send acknowledge to transmitter.

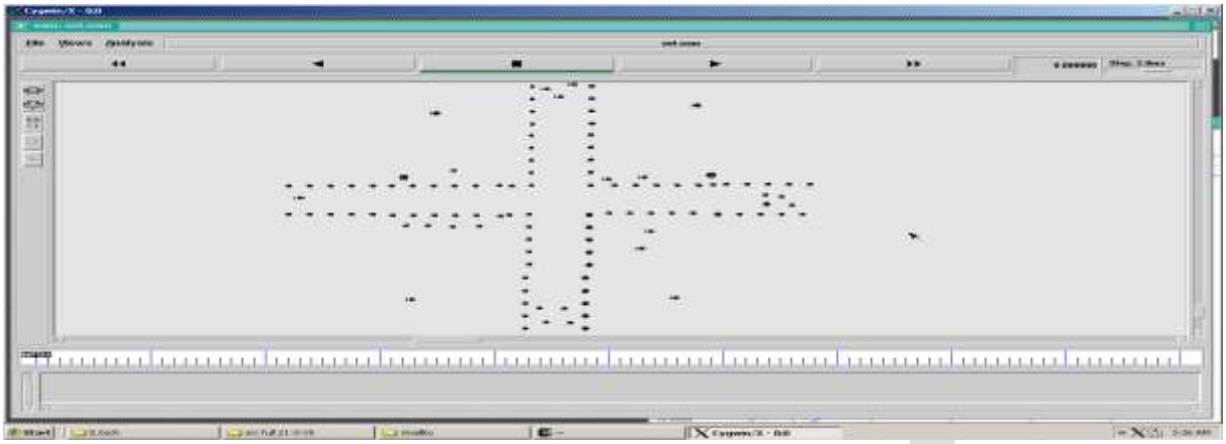

Figure 4.1: Multiple Number of Wireless Nodes Created

This module figure 4.2 is developed to Topology design all node place particular distance. Without using any cables then fully wireless sensor equipment based transmission and received packet data. Node and wireless between calculate sending and receiving packets. The cluster head is at the center of the circular sensing area. Intermediate the sender and receiver of this networking performance on this topology.

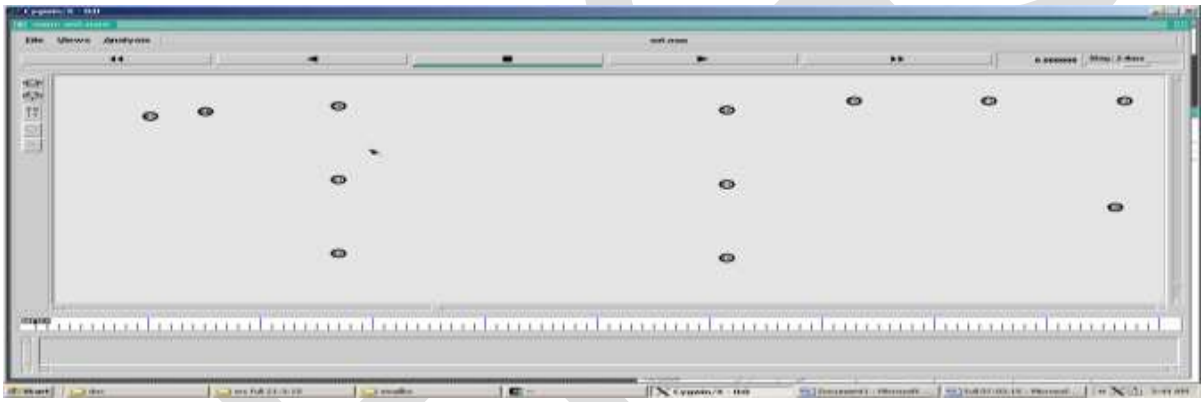

Figure 4.2: Wireless Nodes placed at Particular Distance

Figure 4.3 shows wireless networks to create the no of nodes. the packets to send and receiving through the source to destination. it's based the scheme of packets delivered for ack packet drop on the nodes. in this network to creating the source and destination node of the network and transmit the data to processing on their whole networking.

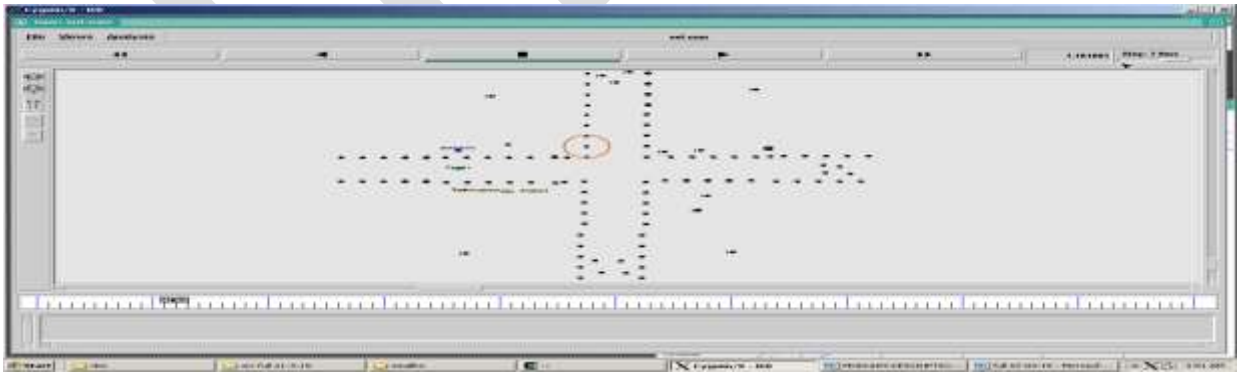

Figure 4.3: RSU can send Information about Transmitting Data

Figure 4.4 shows wireless networks use some sort of radio frequencies in air to transmit and receive data instead of using some physical cables. The most admiring fact in these networks is that it eliminates the need for laying out expensive cables and maintenance costs. Due to the dynamic nature of the clustering formation in the VANET the vehicle nodes are inter related with the

key generation node and thus lead to the security issue, as soon as collusion takes place the cluster head selects another KG node and keying process continues.

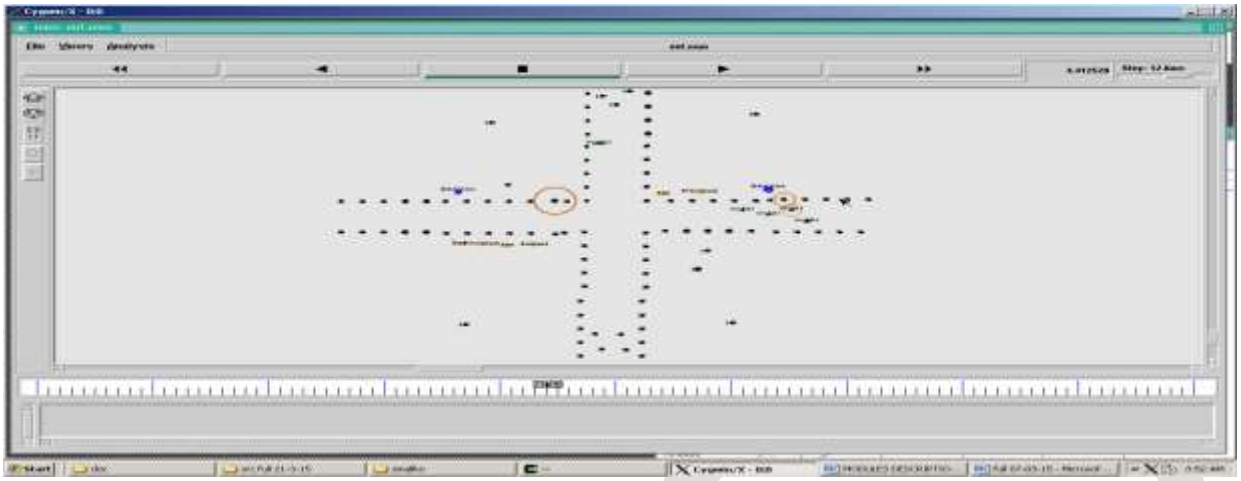

Figure 4.4: Vehicle Nodes are Inter-related with the Key Generation Nodes

This module figure 4.5 shows RSU consider into new way of communication. In this process to maintaining the separate time slot as well as key for every user.

Figure 4.5: Creating New Way Communication using RSU

Vehicular Ad-hoc networks enable vehicles that are not necessarily within the same radio transmission range to communicate with each other. It connects RSU than later connected to the internet, forming a fixed infrastructure that refers then the capability of communicating with each other with roaming vehicles.

This module figure 4.6 computing device located on the roadside that provides connectivity support to passing vehicles.

Figure 4.6: Creation of New Road Side Unit

In this module, figure 4.7 Based on Time Slots the Data can be delivered from Source to Destination. When used the communication networks, such as Ethernet or packet radio, throughput or network throughput is the rate of successful message delivery over a communication channel. The data these messages belong to may be delivered over a physical or logical link, or it can

pass through a certain network node. Throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second (p/s or pps) or data packets per time slot.

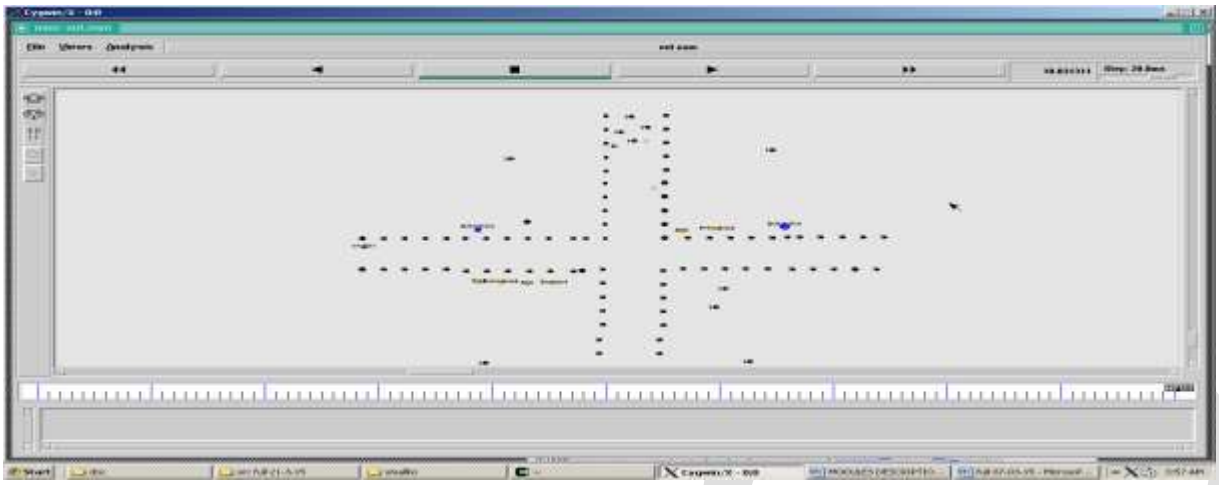

Figure 4.7: Based on Time Slots the Data can be delivered from Source to Destination

CONCLUSION

In this paper we have done , securely data transfer using Diffie-Hellman algorithm in VANET. To perform this algorithm, efficient data transformation. Data will be transferred without any packet loss. Each user have own time slot. In each time slot, all users that are predictable to connect to the RSU are specified. With the use of Diffie-Hellman key exchange it is easy to find out another route quickly in case of false route. To support data transfer in efficient manner high performance networks are required, which impose systematic design on the network to unleash the power of the VANET. Diffie-Hellman algorithm can be used to recover the failure nodes.

REFERENCES:

[1] Balmahoon, R., and R. Peplow. "Vehicular Ad- Hoc Networks: An Introduction to Privacy." Southern African Telecommunication Networks and Applications Conference (SATNAC) will be held from. Vol. 2.

[2] De Castro, Cristina, Carla Raffaelli, and Oreste Andrisano. "A dynamic hierarchical VANET architecture for Named Data Networking applications."*Communications (ICC), 2015 IEEE International Conference on*. IEEE, 2015.

[3] Liu, Kai, et al. "Cooperative Data Scheduling in Hybrid Vehicular Ad Hoc Networks: VANET as a Software Defined Network." (2015).

[4] Z. Chen, H. Kung, and D. Vlah, “Ad Hoc Relay Wireless Networks over Moving Vehicles on Highways,” Proc. ACM Mobihoc, pp. 247-250, 2001.

[5] F. Bai, D.D. Stancil, and H. Krishnan, “Toward Understanding Characteristics of Dedicated Short Range Communications (DSRC) from a Perspective of Vehicular Network Engineers,”Proc. ACM MobiCom, 2010.

[6] Z. Li, Y. Liu, M. Li, J. Wang, and Z. Cao, “Exploiting Ubiquitous Data Collection for Mobile Users in Wireless Sensor Networks,” IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 2, pp. 312- 326, Feb. 2013.

[7] M. Li and Y. Liu, “Traffic Management through Inter-Communication between Cars using VANET System,” IEEE /ACM Trans. Networking, vol. 18, no. 1, pp. 320-332, Feb. 2010.

[8] L. Chisalita and N. Shahmehri, “Distributed Key Management Techniques for Message Authentication in VANETs,” Proc. Fifth IEEE Conf. Intelligent Transportation Systems, pp. 336-341, 2002.

[9] Z. Li, Y. Zhu, H. Zhu, and M. Li, "Compressive Sensing Approach to Urban Traffic Sensing," Proc. IEEE 31st Int'l Conf. Distributed Computing Systems (ICDCS), 2011.

[10] H. Zhu, Y. Zhu, M. Li, and L.M. Ni, "SEER: Metropolitan-Scale Traffic Perception Based on Lossy Sensory Data," Proc. IEEE INFOCOM, 2009.

[11] J. Eriksson, L. Girod, B. Hull, R. Newton, S. Madden, and H. Balakrishnan, "The Pothole Patrol: Using a Mobile Sensor Network for Road Surface Monitoring," Proc. ACM Sixth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys), 2008.

[12] P. Gibbons, B. Karp, Y. Ke, S. Nath, and S. Seshan, "Privacy in Location-based Services: A System Architecture Perspective," IEEE Pervasive Computing, vol. 2, no. 4, pp. 22-33, Oct.-Dec. 2003.

[13] U. Lee, B. Zhou, M. Gerla, E. Magistretti, P. Bellavista, and A. Corradi, "Mobeyes: Smart Mobs for Urban Monitoring with a Vehicular Sensor Network," IEEE Wireless Comm., vol. 13,no. 5, pp. 52-57, Oct. 2006.

[14] I. Leontiadis and C. Mascolo, "GeOpps: Geographical Opportunistic Routing for Vehicular Networks," Proc. IEEE Int'l Symp. World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 1-6, 2007.

[15] G. Marfia, M. Roccetti, C.E. Palazzi, and A. Amoroso, "Secure and Efficient Protocol for Vehicular Ad Hoc Network with Privacy Preservation," Proc. ACM MobiHoc Workshop Pervasive Wireless, 2011.

[16] I. Leontiadis, P. Costa, and C. Mascolo, "Silent Cascade: Enhancing Location Privacy without Communication QoS Degradation," Proc. IEEE INFOCOM, 2010.

[17] A. Balasubramanian, B. Levine, and A. Venkataramani, "A secure anonymous communication scheme in vehicular ad hoc networks from pairings," Proc. ACM SIGCOMM, 2007