Assessment of Different Attacks and Security Schemes in Vehicular Ad-hoc Network

Mahendra Kumar Jhariya
PG. Student
Department of CSE
UIT, RGPV

Piyush Kumar Shukla
Assistant Professor
Department of CSE
UIT, RGPV

Raju Barskhar
Assistant Professor
Department of CSE
UIT, RGPV

ABSTRACT
The concept of VANETs is incorporating data sharing capability and wireless communication. The vehicles are turned in network which provides services that ones used to in offices or homes. VANETs are distinguished from other kinds of ad hoc networks by their hybrid network architectures, node association characteristics, and new application scenarios. VANET uses Road Side Unit (RSU). RSU provides information to the Vehicular Ad Hoc Network users. Every vehicle is interconnected to each other. It sends alert message to another vehicle to decrease or increase the speed to avoid accidents. Security and privacy are essential in vehicular communications for successful reception and use of such a technology. Every vehicular safety application should be tested before it is deployed in a real world to use for. Simulation tool has been preferred over outdoor experiment. It is require that a traffic and network simulator should be used together to perform this test. Security scheme, previously proposed in this paper in the presence of attacker definitely improves the performance of VANET. The revise of different security schemes are provides the suggestion about to propose a new security scheme to secure VANET.

Keywords
VANET, RSU, Security, Attack, Ad-hoc

1. INTRODUCTION
The VANET is a the art of integrating ad hoc network, wireless LAN and cellular technology to achieve Vehicle-to-Vehicle (V2V) Communications also identified as Inter-Vehicle Communications (IVC) and Roadside-to-Vehicle Communications (RVC or R2V).VANETs provide us the valuable concept for improving efficiency and safety of future transportation**[23].** The vehicles or node are mobile, thus a self organized and capable of operating without infrastructure maintain network is needed. The various type of information is provided to the vehicles such as the current speed, location and also services like email, audio/video sharing. These types of network are called Service-Oriented VANET.

IEEE has defined the new characteristics for setting the network i.e. 802.11p or 802.16(WiMax). Communication is provided for small range with less latency. 75 MHz range has been allocated in 5.9 GHz band for DSRC by the USA and also 30 MHz range in the same band for ITS has been allocated by the Europe **[20].** The traffic safety has been the demanding issue in traffic management. To attain this, the vehicles perform as sensors and exchange warnings. If any vehicle is more then the speed limit then other vehicles can launch a warning message to that exacting vehicle, by getting the information the driver get attentive and pedals speed and avoid accidents.

Two modes of communication are there in VANET:

1. Vehicle to Vehicle (V2V) or Inter Vehicle Communications (IVC) communications.
2. Vehicle-to-Infrastructure (V2I) or Roadside-to-Vehicle Communications (RVC or R2V)

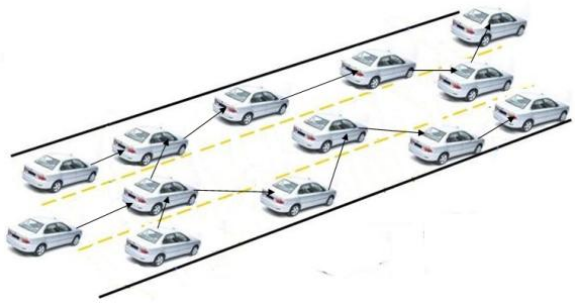

Fig.1. Vehicle to Vehicle communication

First is a pure wireless ad hoc network in which vehicle to vehicle communicates exclusive of any support of infrastructure fig.1. To permit V2V communication, vehicles must form some kind of network, called Vehicle Ad hoc Network (VANET). A VANET is a decentralized and self-organizing network poised of high speed moving vehicles **[8].** V2V provides the short range of vehicular network. Vehicles can exchange a information openly with each other's without passing by the road infrastructure.

Second is communication between and with the the road side units (RSU) fig 2. A fixed infrastructure is used called Road Side Unit (RSU). Each node in VANET is set with two types of unit i.e. On Board Unit(OBU) and Application Unit (AU). OBU has the communicational ability whereas AU executes the program creation OBU‘s communicational capability. RSU is a device which is placed at corner of the road ands its work is to facilitates the user with the necessary information required by the user. It’s main work is to maintain the proper functioning of the network. The RSU’s connects to the internet and also connect the registered user with internet, whenever the vehicles get connected by it nearby RSU. Once a vehicle get registered with any road side unit it information is saved in the database of that road side unit. RSU stores and study the real time vehicles information. These road side unit also communicate with each other through secure channel, so that the information is kept safe. This type of network are referred as service oriented VANET. Such network provides long range of vehicular communication.

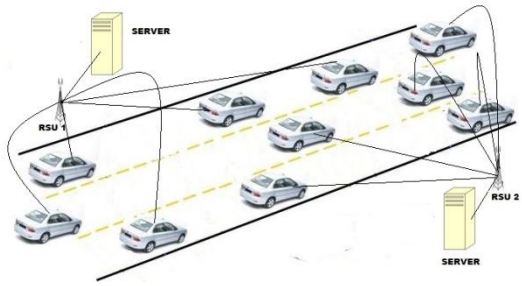

Fig.2. RSU to Vehicle Communication

The Vehicular Ad-Hoc has some of the important benefits which are mentioned below:

1. Warning drivers about the road condition.
2. Find the best available route to destination.
3. Connectivity of the vehicles' to internet while traveling.
4. Communication between the vehicles could be established.
5. The driver could get the help in VANET based network, when encounters some problem,.
6. Vehicular networks have the advantages over the Ad-Hoc network that they do not have critical situation for computational recourses and power consuming .
7. VANET utilizes static infrastructure such as road side base stations.

2. APPLICATIONS OF VANET

The applications of VANET can be categorized into two categories [20].

2.1 Application For Safety

For the vehicles to be safe in the traffic these application are used. It is again classified in following way:

• **Crash Avoidance**: By the detailed study it was analyzed that if the drivers are warned just before the crash, then the accident can be avoided. If a driver gets a warning message/signal on time, then the driver gets alert and collision could be avoided,

• **Supportive Driving:** In the traffic if the driver wants to drive uninterruptedly and safely, then they must be supportive in nature. The signals for traffic related warnings must be shared to each other in the network.

• **Optimizing Traffic:** As the driver are supportive the traffic could be controlled by generating the information signal related to the traffic like jam, accidents etc. to the other vehicles. So that the other vehicle could follow another path without wasting there time.

2.2 Application for User

The user applications are applied for the user other then the safety. These user application are the application related to the entertainment.

• **P2P application:** According to this applications VANET offers the various service among the vehicles in the network.

• **Internet Connectivity:** All the user always wants to be online i.e. every time connected to the internet. In VANET continuous connectivity of the Internet is provided to the user.

• **Extra services:** Now a day's VANET are used for the few other services depending on the user choice eg. payment service to collect taxes, to find the petroleum station, café etc.

3. ROUTING PROTOCOLS IN VANET

Routing protocols are discovering the path and keep routing information in a table previous to the sender starts transmitting data[19]. These are separated into Proactive, Reactive and Hybrid Protocols [7, 8].

3.1 Table Driven /Proactive protocols

The table driven routing protocol commonly known as proactive protocol. The routing information, next forwarding hop is maintained in the background irrespective of requirements for communication. The gain of proactive routing protocol are that the destination route is stored in the background because there is no route discovery. The drawback of this protocol is that it provide low latency in real time application.

3.2 On Demand /Reactive protocols

On-demand protocols are usually known as Reactive routing protocol which decrease the network overhead. When the node want to communicate with each other the reactive routing protocol open the rout. In the rout discovery phase the query packet are flooded into the network for the search of the path which is completed when the route is found.

3.3 Hybrid Routing Protocols

Hybrid routing protocol is a combination of both table driven/proactive and on demand/reactive protocols. The main aim of these protocol is to minimize the control overhead of the table driven protocols and also to min. the delay in the route discovery phase of the on demand protocols. These protocols has the higher scalability then the above mentioned protocols. The most suitable node is used to discover the route. The network node work mutually so the no. of message rebroadcast is also very less.

4. VANET SECURITY

VANET must please a number of security necessities [13]. The security scheme in VANET must satisfy the following:

1. **Authentication:** Authentication means that the users are genuine. In VANET vehicles are dependent on the messages that have been generated by the other nodes in the network. It must be sure that the communication is done by the legal user in the network. So the authentication of the user must be satisfied.
2. **Availability:** Availability does not means that the availability of the user but it means that the message is only available to the Authenticated user in the network. If the information is access by the attacker then it can misguide the user of the network.
3. **Non-repudiation:** Non-repudiation means that a node in the network if generates the message then it must not deny that the message is not generated by the node. It may be difficult to find the origin of the information in case of any collapse.
4. **Privacy:** Privacy of the node must be preserved in the network. It is possible that attacker must be interested in the private information of the node.
5. **Data verification:** Every information that is been transmitted on the network must be verified that it correct.

5. VANET ATTACKERS

For the safety of the VANET it is necessary to find that who can be threat to the network, nature, and there capability for damage to cause in the system. These may be of the following types [7].

• **Insider & Outsider**: Insiders can be distinguished as the genuine user of the system. These type of attacker more dangers in nature. Outsiders are the intruders that are trying to access the network without authentication. They have partial ability to attack the network.

• **Malicious & Rational**: A Malicious attackers is the attacker that has to damage the functionality of the network. these type of attacker aims at malfunction of the whole network. They do not have individual advantage to attack. The Rational attackers are expected as they have the individual return.

• **Active & Passive**: Active attackers are the attackers that create signals/ packet that are to be transmitted in the network. The passive attackers are the attacker that just only sense the network.

6. VANET ATTACKS

VANET is open wireless in nature, here is a number of probable attacks in VANET. The probability for attacks are very high. The major idea of the attacker is to generate harms for legal users, and as a outcome services are not easily reached and thus denial of services. Some of the DOS attacks are mentioned below.

6.1 Distributed Denial of Services(DDOS)

DDOS attack is additional harsh than DOS attack since it is distributed in character. This attacker uses dissimilar position meant for attack to start. It uses dissimilar time slot for transfer the message. The character and the time slot in the message may be different which varies from the vehicle to vehicle in the network[2]. The main aim of the attacker is to down the network so that it is not available for the use. The two potential of DDOS attacks are:

a. V2V

b. V2I (RSU)

6.2 Node Impersonation

Every vehicle in VANET has a unique id and with the help of this id they exchange the information in the network. Each node is identified by this unique id in the network. In this attack the attacker changes his/her identity and act as the real message generator. On receiving the message from the nodes the attacker modifies it for his/her benefit and transmits it into the network.

6.3 Sending False Information

The attacker transmits the bogus information in the network. By this fake information the other vehicles get diverted from there route and the attacker get clear path. The attacker could be any of the user. The main of the attacker is to change the decision of the node in the network. So that the attacker can misguides the node and get down the network.

6.4 ID Disclosure

The attacker in this type of attack captured the ID of the target node and there current location. The attacker generates the malicious code that is been transmitted to the target node and thus collect the required information of the node. The privacy of the target node is effected in this type of attack. The attacker utilizes the RSU for this purpose.

6.5 Sybil Attack

This is one of the curricula attacks because in this type of the attack the attacker generated the message that is been transmitted with the different ID and location. In this way the other vehicles in network understand that the message is genuine and it is been transmitted by the another user of the network [5]. The main task of the attacker is to provide an illusion of many vehicles in network tha are communicating with each other, and they are forced to change there decision.

7. RELATED WORK

G.Archana ,S. Andal [6] discussed MREACT focuses on creation the proposed scheme more scalable in terms of the number of users that can connect to an RSU. M-REACT provides the security for data and scheduling mechanism of RSU divided into number of time slots. In M-REACT that proposes an algorithm that uses the key derivation function in several iterations to strengthen the security of the encrypted message. In the work the author has proposed new scheduling mechanism for the Road side unit. The Time Slot(TS) are allotted for each schedule by the RSU. The user has to connected to road side unit within the time slot. The road side unit collect the user data and caches in the free time slot, before any other user connect to it.

Ayonija Pathre ,Chetan Agrawal, Anurag Jain in [3] discussed the different types of attacks that may be available to VANET. In these attacks the malicious users always try to challenge the networks with their selfish behavior. Adhoc protocols play the main role in VANET but they have size limits and are always smaller than the VANETs. They proposed a scheme that provides solution from DDOS attacks. It was found that network availability has been directly affected in the case of DDOS attacks. In DDOS the attacker has congested the whole traffic by that no vehicle will move forward. Therefore, it's necessary to keep up network accessibility and to develop thrust within the VANET network, so as for the protection applications to be helpful and helpful to road users.

Ram Shringar Raw, Manish Kumar, Nanhay Singh [13] have discussed about the VANET various challenges such as technical and security challenges. Also some major attacks and solutions are also discussed that can be implemented against these attacks. They have compared the solution using different parameters. Lastly the mechanisms that can be used in the solutions are disscussed.

Karan Verma, Halabi Hasbullah , Ashok Kumar, in [7] proposed a defending techniques against DoS attacks. The malicious vehicles are identified with the help of consistent IP address information. The Beacon packets are periodically exchanged by all the vehicles to declare their presences and get aware of the next node. Each node keeps the record of it in there database. If a node observes that they have similar IP address in the network, then this IP addresses are identified as the Dos attackers. The security attacks are going to increase in the future. A DoS attack on the network is elaborated in this paper. The DoS prevention has been developed called "IP-CHOCK" used for the prevention of DoS attack. There is no requirement for special hardware and without exchanging any secret information.

Maurice J. Khabbaz, Hamed M. K. Alazemi, and Chadi M. Assi in [9] proposed the new scheme for Intermittently connected Vehicular Network i.e. Delay Aware Data Delivery(DADD). The complete framework has been suggested in the work. In this work RSU (Road Side Unit) are referred to as the Stationary Roadside Unit (SRU). The SRU transmits the information to high speed vehicles, it also authenticates the vehicles that are newly entering into the network. A mathematical model is developed the author. The operation of the SRU with DADD are characterized in this model. The vehicles transmits the data to the destination with minimal delay delivery. The operation of the SRU with DADD is evaluated under the delay delivery of the packet. The accuracy and validity of the proposed model is verified by extensive simulation conducted. The result show that DADD out performance of this schemes to 36.84%.

Yuan Yao, Lei Rao, and Xue Liu in [22] have proposed two Markov chain models for ACs with different priorities to analyze the performance and reliability of the safety-critical data broadcasting on the CCH under both nonsaturated and saturated conditions in VANETs. It gave the detailed analysis of the PRR and PD by taking AIFS differentiation, virtual collision, the minimum/maximum CW, the retry limit, and the difference among FCP, FBP, and MBP into consideration. Moreover, we leveraged the M/G/1/K queue to model the MAC queue with a finite capacity. Finally, an area partition method to obtain an accurate estimation of the PRR. Performance evaluations show that the analytical analysis results match the simulation results very well. According to the numerical analysis, the results shows that the 802.11p standard broadcast on the CCH in a typical highway scenario can easily satisfy the delay constraints; however, it is difficult to meet the reliability requirements. To increase the reliability of the 802.11p broadcast, it can adjust the system parameters. Extended performance studies also show that the external collision has a primary impact on the PPR, and the hidden terminal problem is the main influential factor in the external collision, which degrades the PRR significantly. Udit Agarwal, Monika Saxena in [19], in this paper has study about the position based routing protocol in the VANET. From privacy point of view position is one of the most important data of any vehicle. There study show that these protocol has not to create and maintain the global route from source to destination, so they have better performance. The study show that these protocol has min. average delay, throughput is better, and also provides the safety in the network.

Ajay Rawat, Santosh Sharma, Rama Sushil in [2] presented the comprehensive study of possible attacks and their possible solutions.

Mushtak Y. Gadkari1, Nitin B. Sambre in [11], makes an attempt for identifying major issues and challenges associated with different vanet protocols, security and simulation tools. In this section we have reviewed existing routing protocols, security issues and simulation tools.

Azzedine Boukerche , Horacio A.B.F. Oliveira, Eduardo F. Nakamura , Antonio A.F. Loureiro, in [4], discuss Localization Systems were studied from the viewpoint of Vehicular Ad Hoc Networks (VANETS) that, showed how GPS receivers, the most common source of localization information in VANETS, can become erroneous or unavailable in a number of situations. Then discussed how these localization inaccuracies can affect most VANET applications, especially critical ones. A number of other localization systems are available to be used by vehicles to estimate their positions: Map Matching, Dead Reckoning, Cellular Localization, Image/Video Processing, Localization Services, and Relative Distributed Ad Hoc Localization. All of these techniques have their pros and cons. It also argue that future localization systems for VANets are likely to use some kind of Data Fusion technique in order to provide position information for vehicles that is accurate and robust enough to be applied in VANet critical applications. It then show how Data Fusion techniques can be used to compute an accurate position based on a number of relatively inaccurate position estimations.

Suk-Bok Lee, Joon-Sang Park, Member, Mario Gerla, and Songwu Lu in [17] introduces noncooperative behavior of selfish or even malicious nodes in real-world scenarios, such a vehicular advertisement system cannot be realized unless proper incentives and security mechanisms are in place. This paper presents signature- seeking drive (SSD), which is a secure incentive framework that stimulates cooperative dissemination of advertising messages among vehicular users in a secure way. Unlike existing incentive systems, SSD does not rely on tamper-proof hardware or game-theoretic approaches but leverages a public key infrastructure to provide secure incentives for cooperative nodes. With a set of ad dissemination designs proposed, we demonstrate that our SSD is robust in both incentive and security perspectives. This paper, proposed a potential and promising application scenario, i.e., the dissemination of commercial advertisements in VANETs. Our advertisement models are based on practical aspects such as advertising intensity and dissemination locality. With both selfish users (incentives) and malicious users (security) into account, we have presented SSD, i.e., a secure incentive framework that stimulates cooperative dissemination of ad messages among vehicular users in a secure way. The SSD employs the concept of virtual cash to charge and reward the provision of advertising service as an incentive for users in the network. By leveraging a PKI, SSD provides various security mechanisms for different types of advertisement models. It has reported extensive performance evaluation results of SSD through analysis and simulation experiments. In particular, they have demonstrated the SSD's robustness in both incentive and security perspectives against various types of attacks, and have showed the effectiveness of our advertisement models.

Adil Mudasir Malla, Ravi Kant Sahu in [1], proposed solution to DOS attacks use more than one lines of defense as to counter attack its (DOS) effect. Due to various defense lines along with the decreasing message retransmission rate mechanism, the solution is good enough in handling any type of DOS attack. Apart from this it also controls network traffic congestion, broadcast storm and delay while propagating emergency warning messages among vehicular nodes even in absence of DOS attacks. In short, it efficiently handles both DOS attacks and network transmissions.

8. CONCLUSION

In VANET every vehicles send and receives the data that has been authenticated. The RSU are used for the exchange of safety messages, and will contain few services messages, e.g. announcing services. All RSU monitor the Vehicles to receive all safety related information so that the safety application achieves their goal. An attacker are those entity who wants to spread false information, interrupt communication, impersonate legitimate nodes, compromise their privacy, or take advantages of the network without cooperating in its normal operation. Under high vehicle densities, problems occur with respect to the reservation of channel for exchange

of safety related information. In this paper we present the study of different security techniques that secure the network. The RSU carefully and controlled the possibilities of attacker infection that are forwarding in network.

9. EXPECTED OUTCOME

An attacker sends multiple false request to a number of victim's in a network, exhausting all of the victim's resources and preventing use by genuine users. In this we proposed a new scheme for detecting the routing misbehavior of attacker. In this work if the conjunction is occurs in a particular position then in that case every vehicular node will generating the traffic jam signals called Congestion Announcement signal to their neighbor and by that the vehicular node will change their route. But attacker node will not continuously transferred the right information about the traffic by that conjunction will occur. Vehicular network could be also used for traffic monitoring. In particular, traffic authorities might be interested in obtaining information about road users so that for example they could get traffic flows to deduce current traffic congestion possibilities and detect potential traffic jams.

10. REFERENCES

[1] Adil Mudasir Malla, R.K. Sahu, "Security Attacks with an Effective Solution for DOS Attacks in VANET", International Journal of Computer Applications Volume 66– No.22, pp. 45-49, March 2013.

[2] Ajay Rawat, S. Sharma, R. Sushil, "VANET: SECURITY ATTACKS AND ITS POSSIBLE SOLUTIONS", Journal of Information and Operations Management, Issue 1, Volume 3, pp-301-304, 2012.

[3] Ayonija Pathre ,Chetan Agrawal, Anurag Jain, " IDENTIFICATION OF MALICIOUS VEHICLE IN VANET ENVIRONMENT FROM DDOS ATTACK", Journal of Global Research in Computer Science, pp.30-34, Volume 4, No. 6, June 2013.

[4] Azzedine Boukerche , Horacio A.B.F. Oliveira, Eduardo F. Nakamura , Antonio A.F. Loureiro, "Vehicular Ad Hoc Networks: A New Challenge for Localization-Based Systems q", Science Direct Elsevier Computer Communications 31 (2008) 2838–2849.

[5] DiYan,Routing and Security in Vehicular Networking, /www.cse.wustl.edu/~jain/cse570-13/ftp/vanets/index.html

[6] G.Archana ,S. Andal , "A Framework for Data Security, Identification and Authentication in VANET", International Journal of Innovative Research in Science, Engineering and Technology Volume 3, Special Issue 3, March 2014, IEEE, International Conference on Innovations in Engineering and Technology (ICIET'14) On 21st & 22, pp. 825-830.

[7] Karan Verma, Halabi Hasbullah , Ashok Kumar, "Prevention of DoS Attacks in VANET", Wireless Pers Commun, pp.95–126, 11 April 2013 Springer.

[8] M. Fiore, J. Harri, F. Filali and C. Bonnet, "Vehicular Mobility Simulation for VANETs," ,pp.301-309, 40th Annual Simulation Symposium (ANSS'07), 2007.

[9] Maurice J. Khabbaz, Hamed M. K. Alazemi, and C. M. Assi, "Delay-Aware Data Delivery in Vehicular Intermittently Connected Networks", TRANSACTIONS ON COMMUNICATIONS, pp1134-1143 VOL. 61, NO. 3, MARCH 2013, IEEE.

[10] Moustafa,H., Zhang,Y.: Vehicular networks: Techniques, Standards, and Applications. CRC Press, (2009).

[11] Mushtak Y. Gadkari1, Nitin B. Sambre, "VANET: Routing Protocols, Security Issues and Simulation Tools", (IOSRJCE) Journal of Computer Engineering, pp. 28-38, 2012.

[12] N.D.Karande, K.K.Kulkarni, "Efficient Routing Protocols For Vehicular Ad-Hoc Network", (IJERT) International Journal of Engineering Research & Technology, 2013.

[13] Ram Shringar Raw, M. Kumar, N. Singh, "SECURITY CHALLENGES, ISSUES AND THEIR SOLUTIONS FOR VANET", International Journal of Network Security & Its Applications (IJNSA), pp. 95-105, Vol.5, No.5, September 2013.

[14] S. Fuchs, S. Rass, B. Lamprecht, K. Kyamakya, "Context-Awareness and Collaborative Driving for Intelligent Vehicles and Smart Roads", 1st International Workshop on ITS for an Ubiquitous ROADS, pp 1-6, 2007.

[15] S. Sesay, J. He and Z Yang, "A survey on Mobile Ad Hoc Network", Information Technology Journal, pp. 168 175, 2004

[16] Shanmuga Priya.S, Erana Veerappa Dinesh.S, "A Novel Approach for Data Acquisition and Handover Scheme in VANET", International Journal of Computer Science and Information Technologies (IJCSIT), pp.1443-1446, Vol. 5 (2) , 2014.

[17] Suk-Bok Lee, Joon-Sang Park, Member, Mario Gerla, and Songwu Lu, "Secure Incentives for Commercial Ad Dissemination in Vehicular Networks" Transactions On Vehicular Technology, Vol. 61, No. 6, pp. 2715-2728, July 2012, IEEE.

[18] Swapnil G. Deshpande, "Classification of Security attack in Vehicular Adhoc network: A survey", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 2, , pp.371-377, March – April 2013.

[19] Udit Agarwal1, Monika Saxena, "Comparative and Behavioral Study of Various Routing Protocols in VANET", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, pp. 769-773, October 2013.

[20] Y. Toor, "VANET: Applications and Related Technical issues", Communications surveys & Tutorials, 3rd quarter, pp. 74-88,vol 10, No 3, 2008, IEEE.

[21] Yong Hao, Jin Tang, and Yu Cheng, " Secure Cooperative Data Downloading in Vehicular Ad Hoc Networks", Journal On Selected Areas In Communications/Supplement, , pp. 523-537, Vol. 31, No. 9, September 2013, IEEE.

[22] Yuan Yao, Lei Rao, and Xue Liu, "Performance and Reliability Analysis of IEEE 802.11p Safety Communication in a Highway Environment", Transactions On Vehicular Technology, Pp. 4198-4212, Vol. 62, No. 9, November 2013, IEEE.

[23] Yuen Liu, Jun Bi, Ju Yang, "Research on Vehicular Ad hoc Networks", 2009 Chinese Control and Decision Conference (CCDC 2009),978-1-4244-2723-9/09/2009 IEEE