Volume 4, No. 6, June 2013
Journal of Global Research in Computer Science
ISSN-2229-371X
REVIEW ARTICLE
Available Online at www.jgrcs.info

# IDENTIFICATION OF MALICIOUS VEHICLE IN VANET ENVIRONMENT FROM DDOS ATTACK

Ayonija Pathre[1] ,Chetan Agrawal[2], Anurag Jain[3]

[1]Department of Computer Science, RIST, Bhopal, M.P., India
ayo.pathre@gmail.com[1]
[2]Profesor, Department of Computer Science, RIST, Bhopal, M.P., India
chetan.agrawal12@gmail.com[2]
[3]Profesor, Department of Computer Science, RIST, Bhopal, M.P., India
anurag.akjain@gmail.com[3]

***Abstract:*** Security is one in all the main problems in VANET. Cooperation among inter-vehicular networks and device networks placed inside the vehicles or on the road need to be further investigated and analysed. As the number of vehicles grows the trust between them should also be maintained for the flexible communication. There are lots of analysis regarding VANET for driving services, traffic data services, user communication and knowledge services. This network, with its huge size, plays a critical role in communication because all types of people use it to achieve daily routine required service. A small error in these can cause great disaster in roads specially. Imagine an attacker take control over a worldwide VANET-based network then he will be able to break it and cause chaos in all roads .VANET will perform effective communication by utilizing routing info. Some researchers' area unit contributed tons within the space of VANET. During this article in the main that specialize in important options, performance improvement, over read of routing protocol and represents the previous work has in hot water conveyance unintended network (VANET).

***Keyword*** - Network Availability, Attack, challenge.

## INTRODUCTION

Vehicular Ad-Hoc Networks (VANETs) are a special class of Mobile Ad-Hoc Networks (MANETs) where nodes self-organize and self-manage information in a distributed fashion. They contain vehicles and/or roadside units that assist within the management of the network Security plays a very important role within the system style with the event of VANETs. Due to the unreliable communications in VANETs, security protocols would like a lot of concerns, like privacy, authentication, and consistency of messages. However, the efficiency was unnoticed before; as a result of previous ways incur important communication overhead. Several Intrusion Detection approaches for conveyance unintentional networks (VANETs) are projected. However, not moving pretend vehicles and vehicles with a plausible quality model aren't thought-about in different approaches. Vehicular Ad-hoc Network (VANET) can be envisaged as the network of moving vehicles act in asynchronous and autonomous fashion. Economical and scalable data disseminated may be a major challenge because of the movement of vehicles that causes unpredictable changes in topology. For people living in developing countries the sheer volume of road traffic is also a daily nuisance. The road traffic conditions have an effect on the protection of the population since one point two million people worldwide are calculable to be killed once a year on the roads. For this reason, these days the motorcar motive business and governments invest several resources to extend road safety and traffic potency, in addition on cut back the impact of transportation on the setting. Two communication modes can be distinguished: the Vehicle-to-Infrastructure (V2I) and Vehicle to Vehicle (V2V) communications. The first mode requires the use of roadside sensors for vehicles to gather information such as traffic signal violation warning. In the second mode, vehicles can communicate directly with each other's without passing by the road infrastructure. The objective is to increase the vehicle safety by relaying required information from vehicle to vehicle. For example, a vehicle detecting an icy road could inform other vehicles like those traveling in the opposite direction and those traveling in the same lane [1].

Road Side Units (RSUs) collect and analyze vehicles' real-time travel information. After that, the RSUs generate traffic information, which contains the average speed of vehicles, vehicle density, and events like a traffic jam. Finally, the RSUs broadcast it to the vehicles in a very comparatively distance. This is suitable for urban traffic environment. Compared with the existing traffic broadcasting systems, it uses RSU to collect, create and distribute traffic messages, and the traffic messages are propagated reliably with data verification mechanism. Therefore, it can capture the real-time traffic information accurately, and meets the requirements of reducing traffic jam and improving road safety. To allow V2V communication, vehicles must form some kind of network, called Vehicle Ad hoc Network (VANET). VANET is a Mobile Ad-hoc Network (MANET) that has vehicles as network nodes. A VANET is a decentralized and self-organizing network composed of high speed moving vehicles [2].

## SPECIFIC CHARACTERISTICS OF VANET

Vehicular ad hoc networks can be considered as a special case of mobile ad hoc networks (MANETs). However, there are several important factors [2], which make this type of networks specific and which allow to treat them as a separate category. Here are the fundamental VANET features:

**1.** Very high dynamics of nodes resulting in fast topology changes.As the communication devices are put in within vehicles, the network nodes are way more mobile and that they move with a lot of high speed. Vehicles are restricted

to maneuver exploitation roads and to abide by the traffic rules, therefore some quality patterns will be discovered and a few statistical quality models for VANET are designed [1].

**2.** Information regarding this position, movement direction, current speed, town map and planned movement mechanical phenomenon of VANET nodes is offered, as a lot of and a lot of vehicles are equipped with GPS devices and navigation systems.

**3.** VANETs have lack of energy constraints, higher machine power and much unlimited memory capability, compared to other ad hoc networks (especially to sensing element networks).

**4.** VANET networks are sometimes of terribly giant size (case of traffic jams) however additionally during aexist in an exceedingly style of several tiny, neighboring networks with a high chance of rending and connection.

**5.** There is a giant diversity of VANET services and applications, and matched communication is a smaller amount necessary than some intelligent broadcast (for example geocast) needed by most safety connected applications.

## SECURITY CHALLENGE IN VANET

VANET poses a number of the foremost difficult issues in wireless ad hoc and detector network analysis. additionally, the problems on VANET security become more challenging due to the distinctive options of the network, like high-speed quality of network entity or vehicle, and extremely great amount of network entities specifically, it's essential to create sure that "life-critical safety" data can't be inserted or changed by an attacker; likewise, the system ought to be ready to help establishing the liability of drivers; however at a similar time, it ought to protect as way as possible the privacy of the drivers and passengers. It is obvious that any malicious behavior of users, like a modification and replay attack with regard to the disseminated messages, might be fatal to alternative users [4]. VANET security ought to satisfy the following needs:-

- **Message Authentication and Integrity:** Message should be protected against any alteration and therefore the receiver of a message should corroborate the sender of the message. However integrity doesn't essentially imply identification of the sender of the message.
- **Message Non-Repudiation:** The sender cannot deny of sent an information message.
- **Entity Authentication:** The receiver isn't solely ensured that the sender generated a message, however additionally has evidence of the liveness of the sender**.**
- **Access Control:** Access to specific services provided by the infrastructure nodes, or different nodes, is decided locally by police. As a part of access management, authorization establishes what every node is allowed to try and do in VANET**.**
- **Message Confidentiality:** The information of a message is kept secret from unauthorized to access it.
- **Availability**: The network and applications ought to stay operational even within the presence of faults or malicious conditions. This means not solely secure however additionally fault-tolerant styles, resilience to resource depletion attacks, further as survivable protocols, that resume their traditional operations when the removal of the faulty participants.
- **Privacy and Anonymity**: Conditional privacy should be achieved within the sense that the user connected info, as well as the driver's name, the license plate, speed, position, and traveling routes at the side of their relationships, has got to be protected; whereas the authorities ought to be ready to reveal the identities of message senders within the case of a dispute like a crime/car accident scene investigation, which may be accustomed hunt for witnesses.
- **Liability Identification:** Users of vehicles are liable for their deliberate or accidental actions that disrupt the operation of other nodes, or the transportation system. Several attacks are known which will be classified depending on the layer the attacker uses. At the physical layer and link layers the attacker will disturb the system either by jamming or overloading the channel with messages. Flooding false messages or rebroadcasting a recent message is also an attainable attack.
- **Jamming**: The jammer deliberately generates interfering transmissions that prevent communication within their reception range. In the VANET scenario, an attacker can relatively easily partition the network, without compromising cryptographic mechanisms and with limited transmission power.
- **Impersonation**: An attacker can masquerade as an emergency vehicle to mislead other vehicles to slow down and yield. An adversary can also impersonate Road Side Units, spoofing service advertisements or safety messages. So an impersonator can be a threat. Message fabrication, alteration, and replay can all be used towards impersonation.

## ATTACKS IN VANET

In VANET, there are some problematic issues most of which are flied around security issues such as data integrity, privacy, and confidentiality. Moreover, there are some issues which can influence the efficiency of VANET such as unpredictable temporary situations (e.g. creating traffic jam because of an accident). The security of VANETs is one of the most critical issues because their information transmission is propagated in open access environments. It is necessary that each one transmitted information cannot be modified by users WHO have malicious goals. Moreover, the system must be able to detect the obligation of drivers while still maintaining their privacy. There are so many different kinds of attacks [3] that we cannot enumerate every possible one. The most obvious attack we can imagine may be an adversary send some false information and try to convince other drivers and the system. Due to the nature of open wireless medium used in VANET, there are a different type number of possible attacks by that the VANET is exposed to. The purpose of the attackers is to create problem for legal users, and as a result services are not readily available, thus denial of service. Some of the attacks are mentioned below.

### *A. Sybil Attack*

In this attack sort, a node sends multiple messages to alternative nodes and every message contains a special fancied supply identity in such some way that the creator isn't proverbial. The fundamental goals of the assaulter are to produce associate illusion to alternative nodes by causation wrong messages and to enforce alternative nodes on the road to go away the road for the advantages of the assaulter [5].

### *B. Node Impersonation*

Impersonation is an endeavor by a node to send a changed version of a message received from the $64000 mastermind for the incorrect purpose and claim the message has come back from the mastermind. To beat this downside, a novel symbol is appointed to every vehicle node in VANET, which can be wont to verify the $64000 message mastermind. Police might use it to spot the motive force because it is related to driver's identity

 

[6]. It's necessary to guard this symbol in order that it cannot be misused by the assaulter.

### C. *Black Hole Attack*

In this problem a node refuses to participate in the network or when an established node drops out to form a black hole. In this all the traffic of the network gets redirected towards a specific node which is actually doesn't exist which results in data lost. The malicious code picks whether to drop a packet to perform a denial-of-service attack or to use its place on the route as the first step in a man-in-the-middle attack [8].

### D. *ID Disclosure*

It is a passive attack. During this attacker send the malicious code to the neighbors of the target node and collects the desired information. They take the ID of the target node and its current location. Due to this target vehicle's ID are disclosed and that they lose their privacy. In this global observer will access their information by observance the route of the target vehicle. For this purpose attacker will use the RSU (Road side Unit).

### E. *Man in the middle attack*

The attacker sits in the middle of the two communicating vehicle and launch this attack. In this type of attacker control all the communication between the sender and the receiver but communicating vehicles assume they are directly communicating with each other [7]. In MIMA attacker listen the communication between the vehicles and inject false or modified message between the vehicles.

### F. *Brute force*

Safety information is crucial in VANET. For secure VANET application as appropriate cryptographic algorithms and approaches. The attacker can use the brute force technique to find the cryptographic key.

### G. *Denial of service (DOS) attack*

In DOS [9] the most objective is to prevent the legitimate user from accessing the network services and from network resources. DOS attack will occur by jam the channel system so no authentic vehicle will access it.In VANET it's most major problem because the user cannot communicate within the network and pass data to other vehicle that could result in a lot of devastation in life important application. 3 alternative ways through offender can do it.

**a.** In basic level the attacker overwhelm the node resource so that it cannot perform other necessary tasks which results in becoming the node continuously busy and not able to do anything else.

**b.** In extended level the attacker jam the channel by generating the high frequency in the channel so no vehicle is able to communicate to other vehicle in the network.

**c.** Drop the packets.

*1) Overwhelm the Node Resources*

In this DOS basic level attack, the goal of the attacker is to overwhelm the node resources such that the nodes cannot perform different necessary and important tasks. The node becomes continuously busy and utilizes all the resources to verify the messages. In fig. 1Node behind the attacker node receives this message.

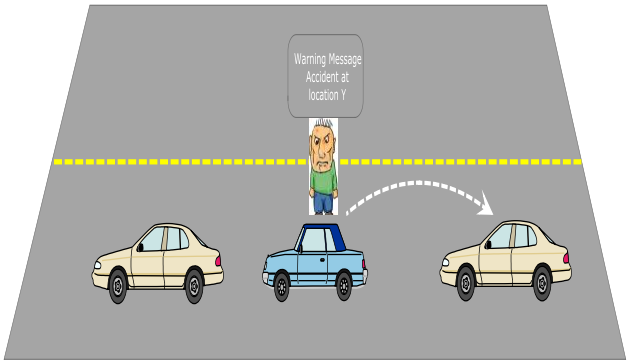


Figure 1. DOS Attack in V2V Communications

However, the sending of identical message is continuously, so keeps the victim node busy and so fully denied for accessing the network.The attacker launches attack to Road Side Unit (RSU) as depicted in Fig.2 When RSU is continuously busy to verify the messages, the other nodes need to communicate with the RSU will not be able to get any response from it, so the service is unavailable. Hence, sending important life info during this situation is full of risk.

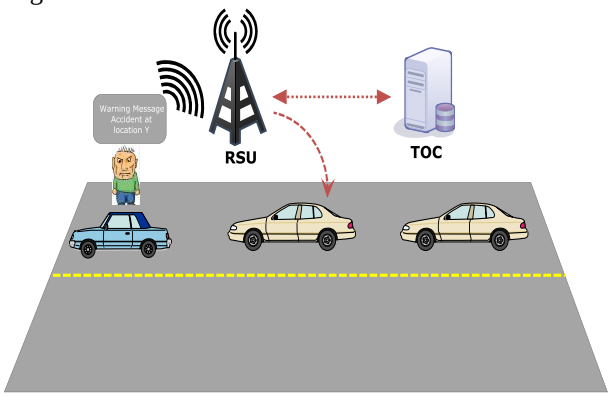


Figure 2. DOS Attack in v2I Communications

*2) Extended Level- Jamming the Channel*

This is a high level of DOS attack within which attacker jams the channel, therefore not permitting another user to access the network. Attacker sends high frequency channel and jams the communication between any nodes in a domain, as depicted in Fig. 3. These nodes cannot send or receive messages in that domain; i.e. services are not available in that domain due to this attack. When a node left the domain of attack, only then it will send and/or receive messages. The next stage of attack is to jam the communication channel between the nodes and the infrastructure. Fig.4.showed the situation where the attacker launches an attack near the infrastructure to jam out the channel, leading to network breakdown. During this way, sending and/or receiving messages to/from different nodes aren't possible and would fail due to network inaccessibility.

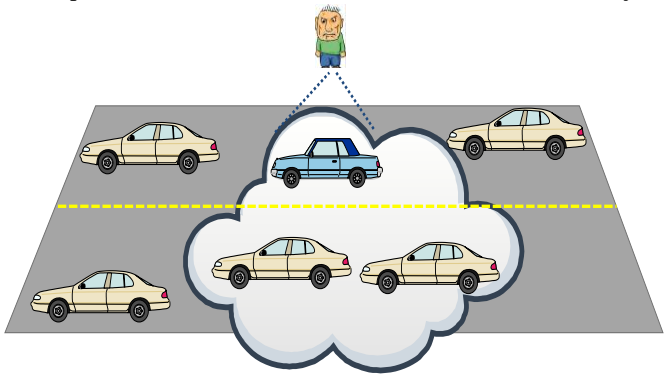

Figure 3. A Domain Of Jammed Channel For V2V Communications

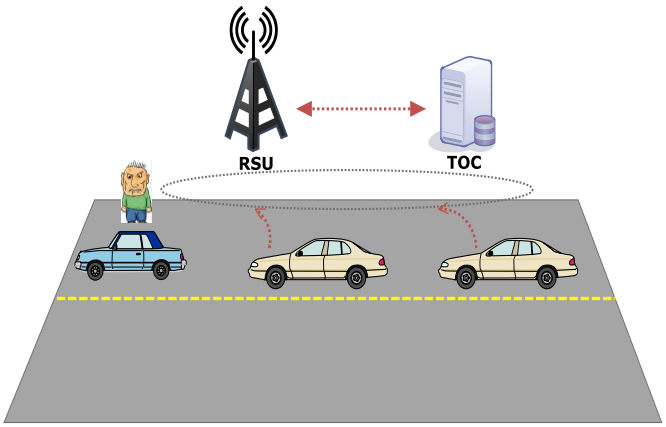


Figure 4. Jam The Channel Between Vehicle-To-Infrastructure

## DISTRIBUTED DENIAL OF SERVICES (DDOS)

DDOS attacks are a lot of severe within the vehicular environment as a result of the mechanism of the attack is in distributed manner where the impact is distributed in the network, in this type of attack, the attackers launch attack from different locations. There are 2 possible cases as follows.

***Case 01***-In these type attacks are launch different time slot and different location. The nature of the messages and time slots may vary from node to node of the attackers. The main aim of the attacks is to achieve network inaccessibility by bringing the network down at a target node. As depicted in Fig. 5, there are three attackers' cars as a node (black color cars) sends some messages to a target node in front (gray color car). After short of time, the target node cannot communicate with the other nodes.

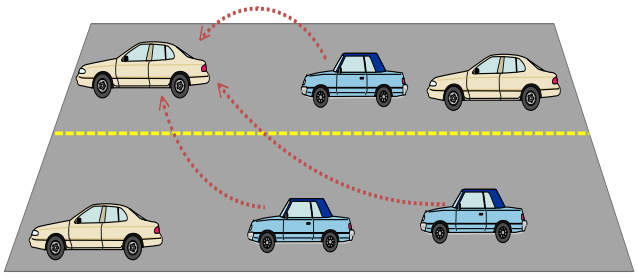

Figure 5. DDOS in V2VCommunications

***Case 02***-In this case, the target of attack is the VANET infrastructure (RSU) as shown in Fig.6There are three attackers in the network and launch attack on the RSU infrastructure from different locations. When another nodes that are in network want to access the network, the infrastructure is overloaded, thus DOS.

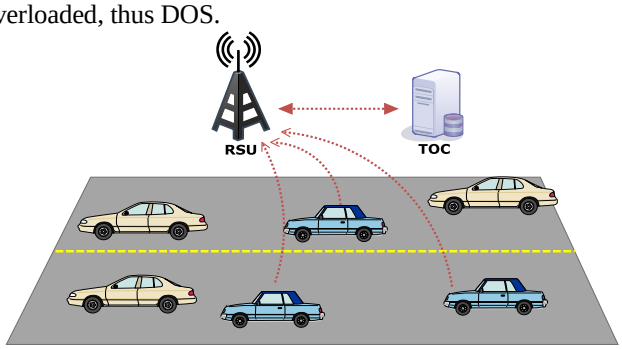


Figure 6. DDOS in V2I Communication

## WORK HAS TO BE DONE IN DIFFERENT AREAS LIKE: SECURITY, TRAFFIC CONGESTION ETC

Paper [10] presents a traffic info aggregation and propagation theme, that is appropriate for the town surroundings and supported Vehicle unexpected Network (VANET) to enhance the traffic condition. Wayside units (RSUs) will collect, produce and distribute traffic messages, victimization vehicle-to-vehicle communication and vehicles mutual cooperation. Compared with the prevailing traffic info systems, this theme will capture the period of time traffic info accurately, and broadcast all traffic info at constant time. Therefore, the vehicles will receive the traffic info that it want in time. During this means, this theme will meet the need of reducing hold up and rising road safety.

In this work [11] a novel security scheme, In SMSS, we tend to specialize in the vehicle-to-vehicle communications, which is among the everyday situations in VANETs. The biradial cryptography is utilized in our theme to make sure the consistency of the messages; the native pseudonyms square measure equipped to safeguard the privacy; and also the preshared keys square measure introduced to implement the authentication. This scheme uses pseudonyms and the symmetric encryption, instead of the traditional public/private one, to satisfy the security needs in VANETs, and thus provides the improvements in the outstanding reduction in security overhead of energy and computational speed, and the efficient privacy protection by pseudonyms. This paper makes a detailed description of the novel scheme, and then analyzes its performance in comparison with that of the PKI security scheme.

V2V routing protocols should be robust, reliable and minimize the latency and the network load. For example, in [12] the routing protocols AODV, DSR, FSR and TORA, are compared and analyzed using a realistic urban road traffic scenarios. The reported results have shown that AODV and DSR outperform FSR and TORA for all studied performance metrics. A comparative simulation study of AODV and GPSR protocols was presented in [13] and reported results have shown serious performance problems of these protocols in VANETs. Two improvements have been investigated to increase their performance when deployed in VANETs. In a recent study [14], DREAM was evaluated for large scale mobile ad hoc networks using the realistic mobility model, Real Mobgen .The reported results show that average latency is less sensitive as the network size increases. In this paper, a performance evaluation of the DREAM protocol for geographic routing in VANETs is presented.

Fabio Picconi et.al. [15] Is proposed another way to deal with the authentication of aggregated data. This proposal can also handle messages that are similar but not same, and nodes receiving multiple messages with similar information to summarize the information in them using only syntactic aggregation. This means that the information of all the messages is retained in separate entries, but can be compressed in precision. The main idea that the authors propose is to challenge the forwarding vehicle to provide probabilistic proof that the aggregated message is authentic and not constructed. We envision that the TPD provides a transmit buffer service where applications place messages to be transmitted. It can be verified by other nodes that this message is authentic and the information contained in it agrees with the aggregation.

## CONCLUSION

Safety related information messages should be transmitted from node to node within the VANET network in reliable and timely

manner. To attain this, secure communication and network avails should be obtained within the VANET started. In this paper we have discussed the different types of attacks that may be available to VANET. These 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.In future we proposed a scheme that provides solution from DDOS attacks. We 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.

## REFERENCES


[1] S. Fuchs, S. Rass, B. Lamprecht and 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.

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

[3] .Farrukh Shahzad, Amir Qayyum, Rashid Mehmood," A Survey on Security in Vehicular Ad Hoc Networks Saira Gillani", Communication Technologies for Vehicles, Springer Berlin Heidelberg, pp. 59-74, 2013.

[4] Tim Leinmuller, Elmar Schoch, and Christian Maihofer, "Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks", Proceedings of Forth Annual Conference on Wireless on Demand Network Systems and Services Oberguyrgl,pp.84-91, 2007

[5] G. Guett, C. Bryce, "Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs)", WISTP 2008, LNCS 5019, pp.106-116.

[6] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, M. Zhendong, F. Kargl, A. Kung, J-P Hubaux, "Secure vehicular communication system : Design and Architecture Communications" IEEE Magazine, November 2008,vol. 46, pp. 100-109.

[7] Li, F., Wang, Y., "Routing in vehicular ad hoc networks: A survey," Vehicular Technology Magazine, IEEE , pp.12-22, vol.2, no.2, June 2007.

[8] M. Al-Shurman, Seong-Moo Yoo and Seungjin Park., "Black hole attack in mobile Ad Hoc networks," presented at the ACM Southeast Regional Conference'2004.

[9] Halabi Hasbullah, Irshad Ahmed Soomro, Jamalul-lail Ab Manan,"Denial of Service (DOS) Attack and Its Possible Solutions in VANET",World Academy of Science, Engineering and Technology, pp.411-415,Volume-65, 2010

[10] Feng Zhang, Jianjun Hao and Shan Le "Traffic Information Aggregation And Propagation Scheme For Vanet In City Environment", IEEE Proceedings of IC-BNMT, 2010.

[11] Lingyun Zhu, Chen Chen, Xin Wang and Azman Osman Lim, "SMSS: Symmetric-Masquerade Security Scheme for VANETs" IEEE Tenth International Symposium on Autonomous Decentralized Systems, 2011.

[12] S. Jaap, M. Bechler and L. Wolf, "Evaluation of Routing Protocols for Vehicular Ad Hoc Networks in City Traffic Scenarios," Proceedings ofthe 5th International Conference on Intelligent Transportation Systems Telecommunications (ITST), Brest, France, June 2005.

[13] V. Naumov, R. Baumann and T. Gross, "An Evaluation of Inter Vehicle Ad Hoc Networks Based on Realistic Vehicular Traces", Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing, 108 – 119, 2006.

[14] M. Bakhouya and N. Cottin, "Performance Evaluation of the Locationbased Protocol DREAM for Large Mobile Ad hoc Networks", In New Technologies, Mobility and Security, NTMS'08

[15] Fabio Picconi, Nishkam Ravi, Marco Gruteser and Liviu Iftode," Probabilistic Validation of Aggregated Data in Vehicular Ad-hoc Networks" Proceedigs if Third International Workshop on Vehicular Ad hoc Network, Los Angeles, California, USA , pp. 76-85, September 2006


 