A Survey on Security Challenges and Threats of Vehicular Adhoc Networks(VANETS)

[1.]Ramachandran. R, [2.]Saravanan. S
[1,2.] Assistant professor, Department of ECE, Peri institute of technology, Chennai, TN, India

***Abstract*— Vehicular Ad Hoc Network (VANET) is a sub class of mobile ad hoc networks. VANET provides wireless communication among vehicles and vehicle to road side equipments. It works without any support from fixed infrastructure, offer a large number of applications. Vehicular ad hoc networks (VANETs) can provide scalable and cost-effective solutions for applications such as traffic safety, dynamic route planning, and context-aware advertisement using short-range wireless communication. This paper, address the security of VANET networks. It provides a detailed threat analysis and devise an appropriate security architecture and also describes some major design decisions still to be made, which in some cases have more than mere technical impli-cations. In this paper provides two major secure routing algorithms which is ID based and Geography based, Depending on the needs, each category has its advantages. ID methods are for sending data to an individual node On the one hand, Geography methods are for sending data to a group of nodes. Secure routing algorithms in VANETs still has a lot of ground to cover. Currently there is no routing algorithm that is designed to be secure and private from the start. There is a need to strike a balance between privacy and security.**

Keywords*— *Vehicular ad-hoc networks (VANET), security, authentication, privacy, non-repudiation, confidentiality, availability, attacks.

I. INTRODUCTION

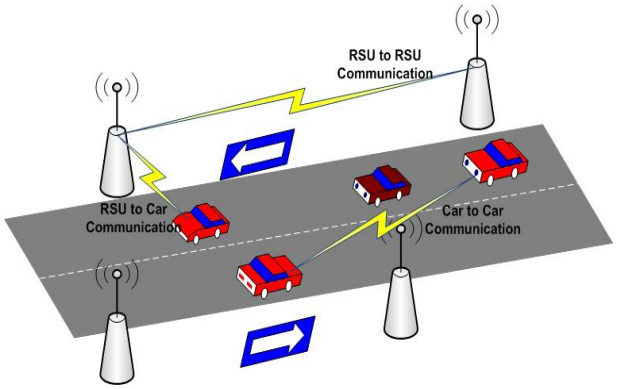
Nowadays, road traffic activities are one of the most important daily routines worldwide. Passenger and freight transport are essential for human development. Thus, new improvements on this area are achieved every day - better safety mechanisms, greener fuels, etc. Driving is one of the most incident factors of traffic safety, so there is a clear need to make it safer. [2]Apart from partially automating this task, reliable driver data provisioning is critical to achieve this goal. An accurate weather description or early warnings of upcoming dangers (e.g. bottlenecks, accidents) [6]would be highly useful for drivers. For this purpose, a new kind of information technology called VANET (Vehicular Ad-hoc NETwork) is being developed.

Vehicular Ad hoc Networks (VANET) is part of Mobile Ad Hoc Networks (MANET), this means that every node can move freely within the network coverage and stay connected. In 1998, engineers from Delphi [11] Delco Electronics System and IBM proposed a network vehicle concept aimed at providing a wide range of applications. The Car2Car Communication Consortium is initiated by six European car manufacturers.

II. VANET ARCHITECTURE

Vehicular Ad Hoc Network (VANET) is a sub class of mobile ad hoc networks. VANET provides wireless communication among vehicles and vehicle to road side equipments. It works without any support from fixed infrastructure, offer a large number of applications. Vehicular ad hoc networks (VANETs) can provide scalable and cost-effective solutions for applications such as traffic safety, dynamic route planning, and context-aware advertisement using short-range wireless communication. VANETs are expected to support a wide variety of applications, ranging from safety-related to notification and other value-added services. Instances where the exchange of safety critical information is significant are highlighted below:

- Lane merging/lane changing at highway intersections
- Blind spots of vehicles
- Hidden driveway collision warning
- Adaptive cruise control and cooperative driving
- Roadway condition awareness



The main system components are the application unit (AU), On Board Unit (OBU) and Road Side Unit (RSU). A VANET is a wireless network that does not rely on any central administration for providing communication among the so-called On Board Units (OBUs) in nearby vehicles, and between OBUs and nearby fixed infrastructure usually named Road Side Unit (RSU). In this way, VANETs combine Vehicle TO Vehicle (V2V) also known as Inter-Vehicle Communication (IVC) with Vehicle TO Infrastructure (V2I)

and Infrastructure TO Vehicle (I2V) communications (see Figure 1).

A. On board unit (OBU)

Each vehicle is equipped with an OBU and a set of sensors to collect and process the information then send it on as a message to other vehicles or RSUs through the wireless medium; it also carries a single or multiple AU that use the applications provided by the provider using OBU connection capabilities. The RSU can also connect to the Internet to another server which allows AU's from multiple vehicles to connect to the Internet.

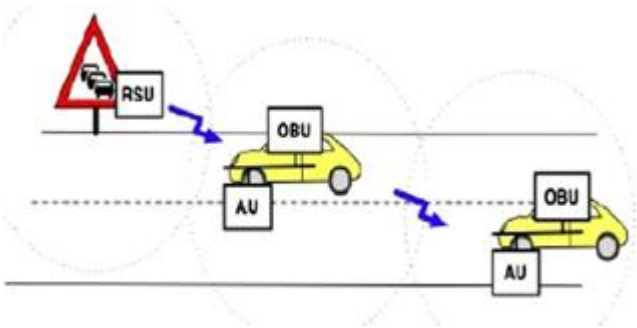


Fig. 2 Vanet Architecture

On the one hand, OBUs in vehicles will broadcast periodic messages with the information about their position, time, direction, speed, etc., and also warnings in case of emergency. On the other hand, RSUs [2] on the roads will broadcast traffic related messages. Additional communications can be also useful depending on the specific application. Among all these messages, routine traffic-related will be one hop broadcast, while emergency warnings will be transmitted through a multi hop path where the receiver of each warning [11] will continue broadcasting it to other vehicles. In this way, drivers are expected to get a better awareness of their driving environment so that in case of an abnormal situation they will be able to take early action in order to avoid any possible damage or to follow a better route.

B. Roadside unit (RSU)

It is foreseeable that VANETs will combine a variety of wireless methods of transmission Technologies such as WAVE, infrared, cellular telephone, 5.9 GHz Dedicated Short-Range Communication [1] (DSRC), WiMAX, Satellite, Bluetooth, RFID, etc. The current state of all these standards is trial use Wireless Metropolitan Area Networks (WMANs), Wireless Local Area Networks (Wireless LANs/WiFi), Wireless Personal Area Network (WPAN), Dedicated Short Range Communications together with their ad hoc mode operation are some wireless technologies for VANET

IEEE802.p protocol is basically used for generating very short range messages for long duration. GPS enabled vehicles are equipped with on board units, which can communicate [6] with each other to propagate information through vehicle to vehicle. DSRC/WAVE operates in 5.9 GHz band (U.S) and 5.8GHz band (Japan, Europe) and has 75 MHz bandwidth allocated for vehicle communication, and range is up to 1 Km with vehicle speed of up to 140 Km/h.

In the future it could be expected that each vehicle will have as part of its equipment: a black box (EDR, Event Data Recorder), a registered identity (ELP, Electronic License Plate), [12] a receiver of a Global Navigation Satellite System like GPS (Global Positioning System) or Galileo, sensors to detect obstacles at a distance lesser than 200 ms, and some special device that provides it with connectivity to an ad hoc network formed by the vehicles, allowing the node to receive and send messages through the network.

III. CHARACTERISTICS AND APPLICATIONS

VANET has its own unique characteristics when compared with other types of MANETs,[3] the unique characteristics of VANET includes, Predictable mobility, High node mobility, No power constraints, Variable network density, Rapid changes in network topology, Large scale network, and High computational ability. There are several general security requirements, such as authenticity, scalability, privacy, anonymity, cooperation, stability and low delay of communications, which must be [7]considered in any wireless network, and which in VANETs are even more challenging because of their specific characteristics such as high mobility, no fixed infrastructure and frequently changing topology that range from rural road scenarios with little traffic to cities or highways with a huge number of communications.

The major characteristics of VANETs are as follows

Characteristics	Details
High dynamic topology	Movement of vehicles at high speed. Suppose two vehicles are moving at the speed of 20m/sec and the radio range between them is 160 m. Then the link between the two vehicles will last 160/20 = 8 sec .
Frequent disconnected network	Frequent disconnection occur between two vehicles when they are exchanging information.
Mobility modeling	Mobility pattern of vehicles depends on traffic environment, roads structure, speed of vehicles, driver's driving behavior and so on.
Battery power	Vehicles battery power and storage is unlimited.
Communication environment	Communication environment between vehicles is different in sparse network & dense network. In dense network building, trees & other objects behave as obstacles and in sparse network like high-way this things are absent. Routing approach of sparse & dense network will be different.
Interaction with onboard sensors	Current position & movement of nodes can easily be sensed by onboard sensors like GPS device. It helps for effective communication & routing decisions.

TABLE 1 major characteristics of VANETs

- **Applications**

After full deployment of VANETs, when vehicles can directly communicate with other vehicles and with the road side infrastructure, several safety and non-safety applications will be developed. [5] Although less important, non-safety applications can greatly enhance road and vehicle efficiency and comfort.

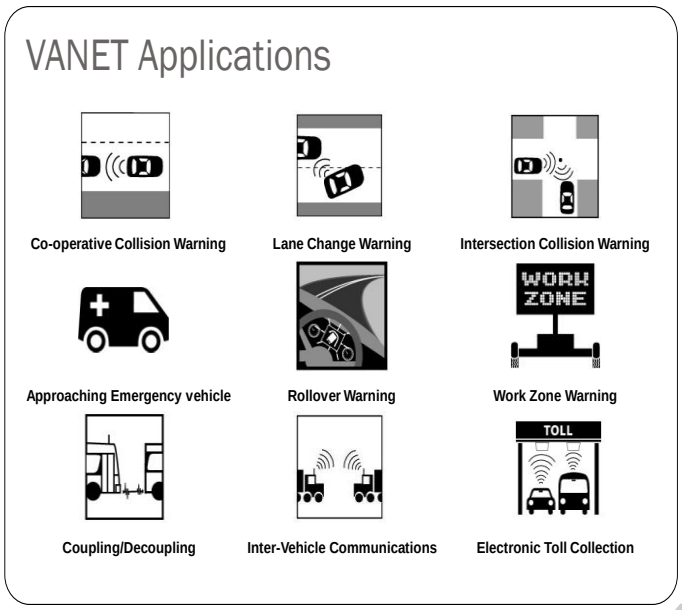


fig. 3 various applications of vanet

IV. SECURITY REQUIREMENTS FOR VANETS

With respect to improving vehicular safety, there is a significant challenge of providing predictable and reliable message delivery in wireless communication channels. Safety information is critical and requires tight latencies and deterministic bounds on propagation delays.[13] A viable accident avoidance system demands rapid and guaranteed availability of localized information to be effective.

VANETs are expected to support a wide variety of applications, ranging from safety-related to notification and other value-added services. However, before putting such applications into practice, different security issues such as authenticity and integrity must be solved because any malicious behaviour of users, [8] such as modification and replay attacks with respect to disseminated traffic-related messages, could be fatal to other users. the exchange of safety critical information is Lane merging/lane changing at highway intersections

A. Authentication:

Vehicle reactions to events should be based on legitimate messages (i.e., generated by legit- imate senders). Therefore we need to authenticate the senders of these messages.

B. Verification of data consistency:

The legitimacy ofmessages also encompasses their consistency with similar ones (those generated in close space and time), be- cause the sender can be legitimate while the message contains false data.

C. Location tracking.

The location of a vehicle in a given moment, or the path followed along a period of time are considered as personal data. It allows building that vehicle´s profile and, therefore, that of its driver[16].

D. Availability:

The availability requirement implies that every node should be capable of sending any information at any time. As most interchanged messages affect road traffic safety, this requirement is critical in this environment. Designed communication protocols and mechanisms should save as much bandwidth and computational power as possible,

E. Non-repudiation:

Drivers causing accidents should be reliably identified; a sender should not be able to deny the transmission of a message (it may be crucial for investigation to determine the correct sequence and content of messages exchanged before the accident).

F. Privacy presevation:

People are increasingly wary of Big Brother enabling technologies. Hence, the privacy of drivers against unauthorized observers should be guaranteed. This requirement is present in all V2V communications. In fact, privacy should not get compromised even if different messages (no matter if under different communication patterns) are sent by the same vehicle. It does not apply to I2V warnings, as the sender (i.e. the infrastructure) does not have privacy needs.

G. Real-time constraints:

At the very high speeds typi-cal in VANETs, strict time constraints should be re- spected. Finally, related to the information itself, data integrity and accuracy must be assured. Both needs are globally referred as data trust. Data at stake should not be altered and, more importantly, it should be truthful.

H. Event data recording (EDR):

Similar to the black boxes on an airplane, EDRs will be used to in vehicles to register all important parameters, especially in situation like accidents

V. SECURITY CHALLENGES

However, most of VANET researches focus on message transmission. Vehicle is extremely personal device; therefore, personal information, so-called privacy has to be protected. In

proposed work in which analyze attacks, problems, and solutions based on topological network model.

A. *Mobility*

In VANETs, nodes moving in high mobility. Vehicles make connection with another vehicles that may never meet before. This connection lasts for only few seconds as each vehicle goes in its direction, and these two vehicles may never meet again.

B. *Bandwidth limitations:*

Another key issue in the VANET is the absence of a central coordinator that controls the communications between nodes, and which has the responsibility of managing the bandwidth and contention operation.

C. *Volatility*

The connectivity among nodes can be in short period of time. Vehicles travelling throw coverage area and making connection with other vehicles. These connections will be lost as each car has a high mobility, and maybe will travel in opposite direction. Vehicular networks lacks the relatively long life context. Personal contact of user's device to a hot spot will require long life password.

D. *Attacks on Privacy*

Attacks on privacy [14, 19] over VANETs are mainly related to illegally getting sensitive information about vehicles. As there is a relation between a vehicle and its driver, getting some data about a given vehicle´s circumstances could affect its driver privacy. These attacks can then be classified attending to the data at risk:

E. *Connectivity:*

Owing to the high mobility and rapid changes of topology, which lead to a frequent fragmentation in networks, the time duration required to elongate the life of the link communication should be as long as possible. This task can be accomplished by increasing the transmission power; however, that may lead to throughput degradation. Accordingly, connectivity is considered to be an important issue in VANET,

F. *Privacy VS Liability*

Liability will give a good opportunity for legal investigation and this data cannot be denied (in case of accidents). On the other hand the privacy must not be violated and each driver must have the ability to keep his personal information from others (Identity, Driving Path, Account Number for toll Collector etc.).

G. *Network Scalability*

No global authority govern the standards for VANET. Standards for DSRC in North America is deferent from the DSRC standards in Europe, Standards for the GM Vehicles is deferent from the BMW.

VI. SECURITY ISSUES AND THREATS

A. *Threats to Availability*

VANETs represent a challenge in the field of communication security, as well as a revolution for vehicular safety and comfort in road transport. [5] In some of the aforementioned applications, messages can influence on driver behaviour, and consequently on road safety. Therefore, the security of communications in VANETs is an essential factor to preventing all these threats.

Threats to Availability	Black Hole Attack
	Malware
	Broadcast Tampering
	Spamming
	Greedy Drivers
	Denial of Service – Consuming the Node Resources; Jamming the Channel; DDoS

1. *Black Hole Attack*

Nodes refuse to participate in the network or when an established node drops out. All network traffics are redirected to a specific node, which does not exist at all that cause those data to be lost. Two proposed possible solutions for this problem in VANETs. Find alternative route to the destination. This solution may impose overload to network. Finding additional node increases unwanted parameters such as delay or cost of service. Exploit the packet sequence number included in any packet header.

2. *Malware*

Malware attacks, such as viruses in VANETs, have the potential to cause serious disruption to its normal operation. Malware attacks are more likely to be carried out by a malicious insider rather than an outsider. Malware attacks may be introduced into the network when the cars' VANET units and roadside station receive software updates.

3. *Spamming*

The presence of spam messages on VANETs elevates the risk of increased transmission latency. The lack of centralized administration causes serious problems in VANET

4. *Selfish Driver*

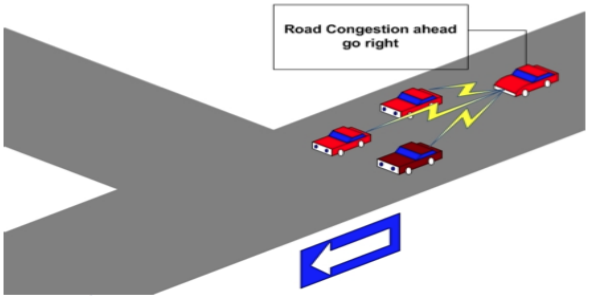


Fig. 4 congestion information sharing in vanet

All vehicles must be trusted to follow the protocols specified by the application. Some drivers try to maximize their profit from the network by taking advantage of the network resources illegally. A Selfish Driver can tell other vehicles that there is congestion on the road ahead. They must choose an alternate route. Thus the road will be clear for him/her.

5. Malicious Attacker

This kind of attacker tries to cause damage via the applications available on the vehicular network. In many cases, these attackers will have specific targets, and they will have access to the resources of the network . For instance, a terrorist can issue a deceleration warning, to make the road congested before detonating a bomb.

6. Denial of Services (DoS)

The goal of is to overwhelm the node resources such that the nodes cannot perform other important and necessary tasks.

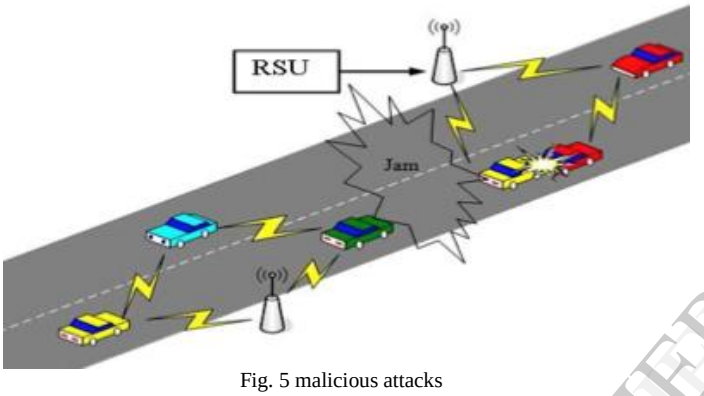


Fig. 5 malicious attacks

B. Threats to Authentication

VANETs represent a challenge in the field of communication security, as well as a revolution for vehicular safety and comfort in road transport.

Threats to Authentication	Masquerading
	Replay Attack
	GPS Spoofing
	Tunneling
	Sybil Attack
	Message Tampering
	ID Disclosure

1. Masquerading

The attacker actively pretends to be another vehicle by using false identities and can be motivated by malicious or rational objectives. Message fabrication, alteration, and replay can also be used towards masquerading. For example, assume an attacker tries to act as an emergency vehicle to defraud other vehicles to slow down and yield.

2. Global Positioning System (GPS) Spoofing

The GPS satellite maintains a location table with the geographic location and identity of all vehicles on the network. An attacker can fool vehicles into thinking that they are in a different location by producing false readings in the GPS positioning system devices. This is possible through the use of a GPS satellite simulator to generate signals that are stronger than those generated by the genuine satellite. This also affects routing in VANETs, especially geographical-based routing

3. Pranksters

People probing for vulnerabilities and hackers seeking to reach fame via their damage . For instance, a prankster can convince one vehicle to slow down, and tell the vehicle behind it to increase the speed

4. Sybil Attack

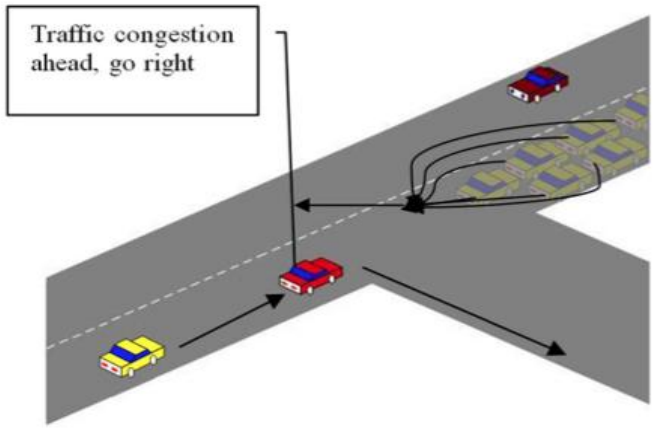
Attacker creates large number of pseudonymous, and claims or acts like it is more than a hundred vehicles to tell other vehicles that there is jam ahead, and force them to take alternate route

5. Message Tampering

Any node acting as a relay can disrupt communications of other nodes. It can drop or corrupt messages, or meaningfully modify messages. In this way, the reception of valuable or even critical traffic notifications or safety messages can be manipulated. An attacker can make this attack by transmitting false information into the network, the information could be false or the transmitter could claim that it is somebody else.

6. Threats To Confidentiality

Because VANET mobility is higher than MANET, routing with capability of ensuring security in VANET is more problematic than Adhoc. Illegal collection of messages by eavesdropping and gathering of location information available through the transmission of broadcast messages. *Location privacy* and *anonymity* are important issues for vehicle users



7. ID Disclosure

This attack discloses the identity of other nodes in the network and tracks the current location of the target node. A global observer monitors the target node and sends a 'virus' to the neighbors of the target node. When the neighbors are attacked by the virus, they take the ID of the target node as well as the target's current location. Rental car companies are using this technique to track their cars

VII. REVIEW OF SECURITY PROPOSALS

In recent years, there have been a plethora of contributions related to VANET security. [11]All those previous works are

based on different techniques to achieve their security goals and so to protect VANETs against the described attacks. In this Section we will analyze the main existing proposals to provide the security services in VANETs.

In particular, we propose location-based group formation according to dynamic cells dependent on the characteristics of the road, and especially on the average speed. [13] In this way, any vehicle that circulates at such a speed will belong to the same group within its trajectory. It is also proposed here that the leader of each group be the vehicle that has belonged to the same group for the longest time According to our proposal, V2V between groups will imply package routing from the receiving vehicle towards the leader of the receiving group, who is in charge of broadcasting it to the whole group if necessary.

- **Secure Routing protocols**

Two major routing categories are ID based Secure Routing algorithm. Geography based Secure Routing algorithm. Depending on the needs, each category has its advantages. ID methods are for sending data to an individual node. Geography methods are for sending data to a group of nodes.

Each security algorithm has its own routing protocols. ID based Secure Routing algorithm has two protocols such as Secure Routing Protocol (SRP) and [9] Secure Beaconing. Similarly Geography based Secure Routing algorithm has two routing protocols that is PRISM and Position-Based Routing. The Secure Routing Protocol Deals with non-colluding malicious nodes, Prevents IP spoofing and ensures privacy. On the other hand Geography based routing algorithm has two protocols, that is PRISM and Position-Based Routing protocol. Here the PRISM Preserves privacy, Avoids creation of pseudonyms (expensive). The another protocol Position-Based Routing provides two levels of encryption. So these proposed security algorithms will show that they protects privacy and analyzes their robustness, and will carry out a quantitative assessment of the proposed solution.

VIII. CONCLUSION

This paper provides a comprehensive survey dealing with all the issues facing VANET, in particular, architectures components, communication domains, wireless access technologies, characteristics, challenges and requirements, applications and simulation tools. Nowadays, vehicular networks are being developed and improved. Several new applications are enabled by this new kind of communication network. However, as those applications have impact in road traffic safety, strong security requirements must be achieved. finally various attacks in VANET have been classified depending on the availability, authentication,
confidentiality, privacy, non repudiation and data trust. It has been observed that the classification helps to deal with different types of attack on routing protocols in VANET. Since attack creates a more severe condition, it is necessary to analyze the effect of attack on routing protocols which makes more secure vehicular environment. Secure routing algorithms in VANETs still has a lot of ground to cover. Currently there is no routing algorithm that is designed to be secure and private from the start. There is a need to strike a balance between privacy and security.

REFERENCES

[1] N.H.T.S. Administration. Vehicle safety communications project task 3 final report, identify intelligent vehicle safety applications enabled by dsrc. Technical Report, US Department of Transportation. Technical Report DOT HS 809 859 2005.

[2] Al-Doori M. Directional routing techniques in vanet. PhD thesis; November 2011. Artimy M, Robertson W, Phillips W. Connectivity in inter-vehicle ad hoc networks. In: Canadian conference on electrical and computer engineering, IEEE, vol. 1;2004. p. 293–8.

[3] Artimy M, Phillips W, Robertson W. Connectivity with static transmission range in vehicular ad hoc networks. In: Proceedings of the 3rd annual communication networks and services research conference. IEEE; 2005. p. 237–42.

[4] Buchenscheit A, Schaub F, Kargl F, Weber M. A vanet-based emergency vehicle warning system. In: Vehicular networking conference (VNC), IEEE, IEEE, 2009;2009. p. 1–8.

[5] Jakubiak J, Koucheryavy Y. State of the art and research challenges for vanets. In: Consumer communications and networking conference. CCNC 2008. 5th IEEE; 2008. p. 912–6.

[6] Jiang D, Delgrossi L. Ieee 802.11p: towards an international standard for wireless access in vehicular environments. In: Vehicular technology conference. VTC Spring 2008. IEEE; 2008. p. 2036–40.

[7] Nekovee M. Sensor networks on the road: the promises Moustafa H, Zhang Y. Vehicular networks: techniques, standards, and applications.CRC Press; 2009. and challenges of vehicular ad hoc networks and grids. In: Workshop on ubiquitous computing and e-Research; 2005.

[8] Freudiger, J.; Raya, M. & Hubaux, J.-P., (2009), Self-organized Anonymous Authentication in Mobile Ad Hoc Networks, *Proceedings of the Conference on Security and Privacy in Communication Networks (Securecomm)*, pp. 350-372, Athens, Greece, September 2009

[9] Füßler, H.; Schnaufer, S.; Transier, M. & Effelsberg W. (2007). Vehicular Ad-Hoc Networks: From Vision to Reality and Back. *Proceedings of the Fourth IEEE/IFIP Annual Conference on Wireless On demand Network Systems and Services (WONS)*, Obergurgl, Austria, January 2007

[10] Gehring O. & Fritz, H., (1997), Practical results of a longitudinal control concept for truck platooning with vehicle to vehicle communication, *Proceedings of the 1st IEEE Conference on Intelligent Transportation System (ITSC'97)*, pp. 117–122, Boston, USA, November 1997

[11]Duri, S., Gruteser, M., Liu, X., Moskowitz, P., Perez, R., Singh, M., et al. (2002). Framework for security and privacy in automotive telematics. *International Workshop on Mobile Commerce* (pp. 25-32). Atlanta, Georgia, USA: ACM.

[12] G. Samara *at al.*, Security Analysis of Vehicular Ad Hoc Networks (VANET), 2010 Second International Conference on Network Applications, Protocols and Service, 2010.

[13] F. Sabahi, The Security of Vehicular Adhoc Networks, Proc. Of the 2011 3rd International Conference on Computational Intelligence, Communication Systems and Networks, 2011.

[14] B. Paul et al., VANET Routing Protocols: Pros and Cons, Int'l Journal of Computer Applications (0975 – 8887), Vol. 20(3), April 2011.

[15] F. Dotzer, Privacy Issues in Vehicular Ad Hoc Networks, BMW Group Research and Technology, 2005.