Security Challenges And Implementation Mechanism For Vehicular Ad Hoc Network

Mostofa Kamal Nasir, A.S.M. Delowar Hossain, Md. Sazzad Hossain, Md. Mosaddik Hasan, Md. Belayet Ali

Abstract: - Vehicular Ad Hoc Networks (VANET) is an emerging and promising technology, this technology is a fertile region for attackers, who will try to challenge the network with their malicious attacks. The security of VANET has mostly directed the attention of today research efforts, while comprehensive solutions to protect the network from adversary and attacks still need to be improved, trying to reach a satisfactory level, for the driver and manufacturer to achieve safety of life and infotainment. We discuss the need for robust VANET networks which is strongly dependent on their security and privacy features. VANET facing many challenges that been addressed in this research, we also discuss a set of solutions presented for these challenges and problems; and we made critics for these solutions.

Index Terms: - VANET, MANET, PKI, VLP, EPKI, EDR, ECC, PCKS

1 INTRODUCTION

VANET is a new type of network which is expected to support a huge spectrum of mobile distributed applications that operated in vehicles. The most significant services in VANET on the roads are that it can give drivers safety in driving. VANET can disseminate useful information about road and traffic situation as well as other noticeable information for people who drive in the range of the typical road. VANET is part of Mobile Ad Hoc Networks (MANET), this means that every node can move freely within the network coverage and stay connected, each node can communicate with other nodes in single hop or multi hop, and any node could be Vehicle, Road Side Unit (RSU). VANET is differing from MANET in a way that nodes in VANETs have improved processing and storage capabilities. Hence with perpetual increase in concentration of vehicles on roads and the ability to communicate over wireless medium, VANETs an inspiring platform for Intelligent Transportation Systems (ITS) for better and safer commuting.

- ***Mostofa kamal Nasir*** *is working as an Asstant Professor of the Department of Computer Science and Engineering of Mawlana Bhashani Science and Technology University, Santosh, Tangail, Bangladesh. Email: kamal.mostofa@gmail.com*
- ***A.S.M. Delowar Hossain*** *is working as an Asstant Professor of the Department of Computer Science and Engineering of Mawlana Bhashani Science and Technology University, Santosh, Tangail, Bangladesh. Email: uzzal35@yahoo.com*
- ***Md. Sazzad Hossain*** *is working as an Asstant Professor of the Department of Computer Science and Engineering of Mawlana Bhashani Science and Technology University, Santosh, Tangail, Bangladesh. Email: sazzad_101@yahoo.com*
- ***Md. Mosadddik Hasan*** *is working as an Asstant Professor of the Department of Computer Science and Engineering of Mawlana Bhashani Science and Technology University, Santosh, Tangail, Bangladesh. Email: shohug_0301012@yahoo.com*
- ***Md. Belayet Ali*** *is working as an Asstant Professor of the Department of Computer Science and Engineering of Mawlana Bhashani Science and Technology University, Santosh, Tangail, Bangladesh. Email: belayet_2003@yahoo.com*

ITS applications have three broad categories such as safety, non safety and infotainment. These applications further categories to accidents, intersection, road congestion, user application, internet connectivity and peer-to-peer application. The security of VANETs is one of the most decisive issues because their information is broadcast in open access environments. It is necessary that all transmitted data cannot be injected or changed by users who have malicious goals. Moreover, the system must be able to detect the obligation of drivers while still maintaining their privacy. These problems in VANET are difficult to solve because of the network size, the speed of the vehicles, their relative geographic positions, and the randomness of the connectivity between them. It is critical for VANET to meet robust security policy to ensure users about issues that can make them worry. VANET security should satisfy four goals, it should ensure that the information received is correct (information authenticity), the source is who he claims to be (message integrity and source authentication), the node sending the message cannot be identified and tracked (privacy) and the system is robust [1]. To guard against misuse activities, the overall organization for VANET security architecture must be carefully designed especially when it is a worldwide implemented in VANET. Our paper presents in section 2 Security of VANET in section 3 types of attack in VANET, in section 4 VANET security challenges, in section 5 security mechanism of VANET which is followed by conclusion.

2 VANET SECURITY

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 all transmitted data cannot be injected or changed by users who have malicious goals. Moreover, the system must be able to detect the obligation of drivers while still maintaining their privacy. These problems in VANET are difficult to solve because In terms of security implementation, there are several layers which are used in proposed protocols to deploy security policies but one of the most often-used levels is layer three for implementation security [2]. There are several methods to assure security in the network world which are also applicable in wireless networks. An overview of 802.11p protocol's Media Access Control layer and the location of security sub-layer are illustrated in Figure 1. Thus, most of protocol implementers prefer using cryptography schemes such as public key. In addition, there are other standard solutions for meeting

security patterns as IPSec for ensuring other aspects of security. The main idea of the security issue besides trust is allowing each car to constitute a local communication area around itself . In this way, each car can exchange vital signs with the neighboring vehicles. Security in VANETs can be improved only after experiencing and issuing models as

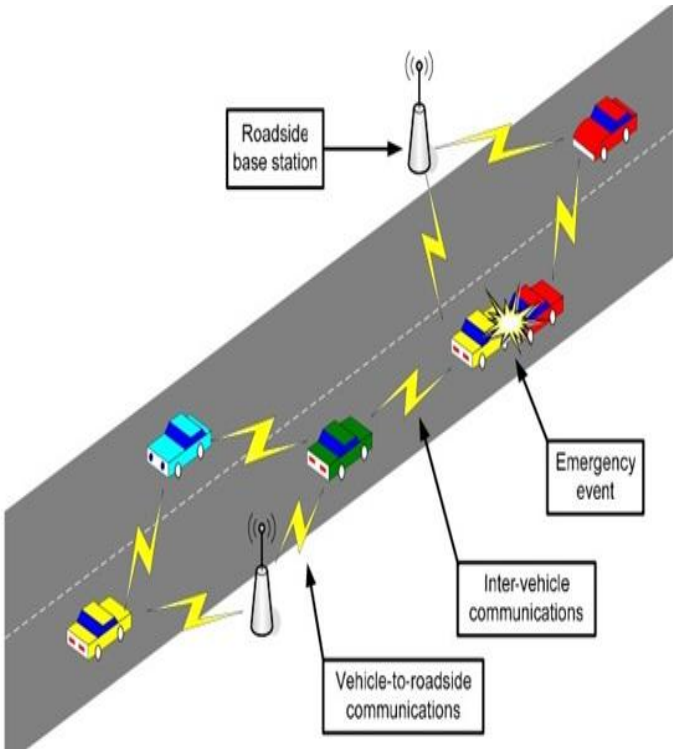

Fig-1: Overview of VANET security

discussed in [3]. First of all, the attacker must be identified and the main principles that guide his attack and for this reason we use basic assumptions about the attacker based on what we can observe as damage from the attack.

3 TYPES OF ATTACK

First of all it is necessary to identify the threats that exist in VANET's and the way those threats can affect the performance and the integrity of the network. Describing threats and certain attacks can be of real use when thinking about the practical and theoretical solutions of these problems. Therefore we categorize security threats into three groups according to the application type that they target according to the works like [4], [5], [6] and [7]. Possible attacks in the network can be various types, active, passive, control of movement, falsification of data etc.

3.1 Classification Based on Nature

Depending on the nature attacks can be classified according to fig. 2.

- **Active vs. passive:** An active attacker is a node that can generate packets and placing on the network, while passive one is that can only push the message in the network. **False information:** Attackers are spread wrong information in the network to influence the behavior of other vehicles [8].

- **False position:** Attackers use this technique of attack to alter the fields related to their position, speed, and direction of travel by broadcast messages. In the worst case, the attacker can clone other vehicles, hiding in this way their presence in case of accidents, and avoiding any responsibility [9].

- **Vehicle tracking:** This is the scenario of like big brother, where a global observer can control the routes of the vehicles designated to use and the observed data for various purposes (for example, some companies that rent cars can trace their cars). To make such a control the "global observer" could control infrastructure such as roads or vehicles in a given geographical location. In this case, the attack is the passive type. We assume that the attacker does not use cameras or devices for tracking physically of a vehicle which wants to discover the identity. This assumption is made to create a scenario feasible in terms of manufacturing cost even if the application of devices such as cameras would give considerable aid to the controls of vehicles.

- **Internal vs. external**: Any attacks by internal nodes are part of the network. This means that the attacker node is a member of the network. Whereas any attacks by external nodes is considered by the network as an intruder. Generally attacks by internal nodes are most effective as they treats authenticated by the network.

- **False GPS signal:** The vehicles that use GPS are easily vulnerable to various attacks such as the GPS signal.

- **Denial of service:** In this style of attack a node may want to block the services offered by VANET or even may want to cause an accident. Examples of attack can be flooding the network with fake messages or blocking transmissions in the network itself. This kind of attack has no intention to make profit by the malignant node.

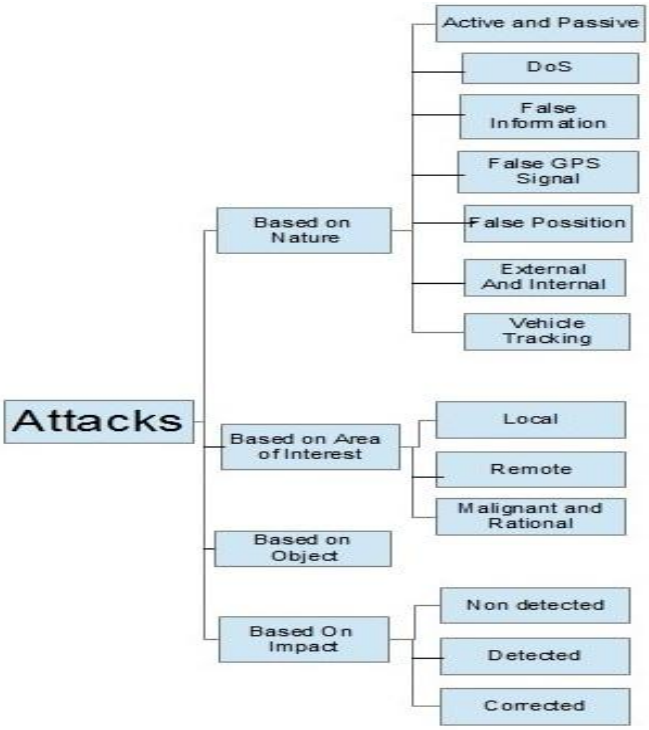

Fig.2: Classification of the attacks in VANET

An example of attack in VANET shows in Figure 3. In this figure two vehicles A2 and A3 enter false information within a network for changing the flow of traffic of the road and obtain a useful result.

3.2 Classification of attacks according to the region

Attacks based on the area of interest are those attacks based on geographical data. We define the attack nodes of an area of interest by "victim nodes ". The area of interest may be limited or extended. Characteristic of this kind of attack is the potential expansion of the infected areas where there is the presence of data corrupted by malicious nodes. The expansion can take place in peripheral area when one or more infected node passing bogus information into another area.

- **Local attacks:** Attackers unleashed by malicious nodes to neighboring nodes by sending false data in order to change the status of evaluation and decision of victim node. Such attacks can be very effective located in the vicinity of one or more malignant nodes. The victim node cannot make comparisons with other nodes in the network; therefore unable to test the veracity of the received data is valid.

- **Remote attacks**: Attackers are attacks to targets node that is distant from the malicious node. The message sending by attackers node contain the fake information, it can arise conflict on a qualitative level between the message and the received message by neighboring nodes to a target node.

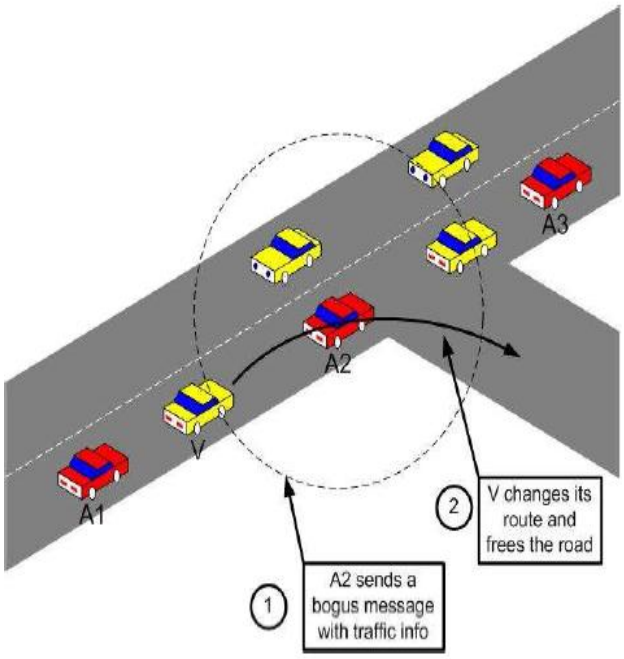

Fig.3: Attack with false information A2 and A3 disseminate false information to influence network.

- **Rational vs. evil:** A malicious attacker does not seek personal benefits from attacks that push into network. This attack in the network does not consider the financial benefits; in contrast to a rational attacker seeks personal profit. To gain a personal profit, a rational attacker much more predictable than a malicious attack in terms of goals and objectives.

3.3 Classification of attacks according to the objectives

They may be also guided by well-defined objectives. The objectives can be traffic control in a given area, the control of vehicle movement, the induction to change the trajectory of vehicles, blocking a service or even block all the services offered by the VANET.

3.4 Classification of attacks based on Impact

The attacks may have different impacts depending on the technique and technology that the attacker uses. The classification according to the impact is as follows:

- **Non Detected:** Attack is not detected by the target nodes. A target node cannot detect an attack if it is isolated or completely surrounded by the malignant nodes. It continuously transmits false information and a victim node accepts incoming fake messages. But as soon as the victim node is in the vicinity of an honest node, can re-evaluate the integrity of the data receive so far and then correct the message.

- **Detected:** Attack detected by the target nodes. A victim node can detect an anomaly attack, because of the small amount of available correct data, remains in doubt about the contents of the receive data. This doubt remains until it encounters a sufficient number of honest nodes that provide a sufficient amount of information for a correction of the data.

- **Corrected:** A node detects a malicious node due to the data received from node that are in contradiction with the data of observations by honest nodes. Some nodes have the opportunity to correct the false messages, in addition to identifying the malicious node.

4 VANET Security Challenges

VANETs will be the largest real-life instance of a self-organized ad- hoc network if implemented correctly. Thus, its size will be of millions of nodes that each has certain properties and can be divided in categories: like authorities, normal cars, service providers, attackers, etc. The main problem for such a large-scale network is the scalability, mostly because these types of problems should be solved in a way transparent to the driver (the normal node in such a network). Besides scalability issues, one of the most important aspects that have to be taken in consideration is the dynamics of such a network. Most of the important attacks target the different forms of privacy that a normal user of the VANET [10] and [11]. Thus, one of the major consumer concerns about this type of communication is the potential influence on privacy. People are usually skeptical about the exchange of information from persons the already know, but from strangers on a highway. Although there are solutions that can offer the possibility of providing the driver and the vehicle anonymity, this may negatively affect the liability of the network. Another key element is a security system is trust [12]. This is particularly emphasized in vehicular networks because of the high liability required from safety applications. Because of the large number of independent network members and the presence of human factor, it is highly probable that misbehavior will arise. Another important factor is that

consumers because highly concerned about their privacy [13]. Drives do not make an exception; therefore the level of trust in vehicles as well as service providers will be low. Also, besides driver and service providers there will be a considerable presence of governmental authorities in such network. Because of the skepticism of most members in such network, the trust in these authorities will be only partial. Cost is another important aspect in the deployment of inter-vehicular communications . The first cost that we encounter in the deployment of such network is the introduction of new communication standards for vehicular communication that will require manufacturers to install new hardware modules on all vehicles, thus increasing the cost of the consumers. Also, another cost is the one for the inter-vehicular communication: mostly it the communication is based on text messages through GSM service. Another important cost is the permanent technical support for the hardware installed on the roads. Last important cost is for the infrastructure that will allow vehicles to access online authorities as part of security services. The time span of inter-vehicular communication until it reaches considerable penetration is around a decade. This means that only a small proportion of vehicles will contain the enhanced features of inter-vehicular communication over the next couple of years. The gradual deployment is an important factor that has to be taken in consideration also from the security point of view.

5 SECURITY MECHANISM OF VANET

5.1 Requirement

- **Authentication**: Vehicle reaction to events should be based legitimate messages. Therefore we need to authenticate the senders of the messages.

- **Verification of data consistency:** The legitimacy of messages also encompasses their consistency with similar ones, because the sender can be legitimate while the message contains false data

- **Availability:** Even assuming a robust communication channel, some attacks can bring down a network. It is very important to point out that the network cannot be brought down, and if the VANET is brought down it can be restored through another way.

- **Privacy:** people are increasingly wary of "The Big Brother Phenomenon" and also about the privacy of such networks.

- **Real time constraints:** At the very high speeds typical in VANETs, strict time constraints should be respected Security Mechanism

- **Electronic License Plates (ELP):** ELPs are unique cryptographically verifiable numbers that will be used as equivalents of traditional license plates. The advantage of ELPs is that will automate the paper-based document of checkup of vehicles. These types of license plate maybe issued by governmental transportation authorities. Hence, the authorities should have the cross- certification agreements that will allow them to verify the ELPs issued by the other authorities.

- **Vehicular PKI**: A public key infrastructure, also known as PKI is the typical architecture used for networks where the presence of online authorities is not always guaranteed. Given the properties of large scale and initially low penetration of vehicular communications infrastructure, a PKI is a good choice for enabling inter-vehicular communication [14]. There are some problems that can occur while using this type of architecture, although it seems very convenient for VANETs. The first problem is the key distribution; another problem is the certificate revocation by which the CA invalidates some private/public keys pairs due to their discovery by an attacker.

- **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

- **Tamper proof hardware**: Vehicles will store cryptographic material such as ELPs and VPKI private or public keys in tamper-proof hardware that will keep this material safe from attackers, thus decreasing the possibility of information leakage.

- **Data correlation**: The bogus information attack cannot be easily discovered, like other attacks like DoS ones. The main solution to this problem is to use data correlation techniques that will collect data received from different sources and thus allowing the vehicle to make a decision on the level of credibility, consistency and relevance of the received information.

- **Secure positioning**: There is a real need for secure position verification, thus vehicles or base-stations may want to verify the position of other vehicles or base-stations "on the fly". The most common solution for this issue is the GPS system that is very convenient but also has a lot of security leaks.

5.2 Privacy and Authentication:

Drawing from the analogy with existing administrative processes and automotive authorities a large number of certificate authorities (CAs) will exist. Each of them is responsible for the identity management of all vehicles registered in its region. The deployment of secure vehicular communication is also influenced by the hierarchical structure within each CA and cross-certification among CA (secure vehicular communication could still be handled locally to a great extent). At the same time, vehicles registered with different CAs can communicate securely in the network as soon as they validate the certificate of one CA on the public key of another CA. The deployment of such networks emphasize that CA manages long- term identities, credentials and cryptographic keys for vehicles. As a basic guideline that can be found in [15], processes and policies for privacy protection should be defined, with minimum private information disclosure on a need-basis and fine-grained control mechanisms for regulating private information disclosure. Nonetheless, signed messages can be trivially linked to the certificate of the signing mode: thus, the removal of all information identifying the user from node certificate does make communication anonymous[16]. Yet, as

the vehicle can change pseudonyms, linking messages signed under different pseudonyms becomes increasingly difficult over time. The change of a pseudonym should be accompanied by a change of the node identifiers used by underlying networking protocols.

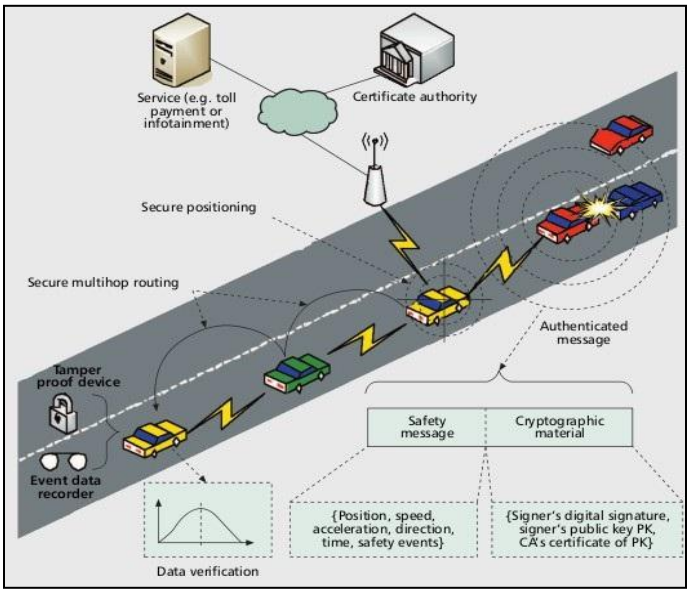

Fig.4: Security Mechanism of VANET

If such identifiers do not change along with the pseudonym, messages generated but a node could be trivially linked according to the address used by the node's hardware and software. On the other hand, the network operation may require that node identifiers remain unchanged for a specific period of time. This implies that a change of pseudonym would be ineffective and thus meaningless throughout the period a protocol identifier must remain changed.

5.3 Security Analysis

Authentication of message legitimacy is provided by the digital signature of the sender and the corresponding CA certificate. The only guarantee that this provides is that the message comes from a vehicle that was trusted, at least when the keys were issued. Availability can be totally guaranteed. Even though the availability of vehicles and the network is almost totally guaranteed, the ways in which an attacker can disrupt the network service are limited: outsiders can only mount jamming attacks. Starting from the initial assumptions we have the following facts: Vehicles cannot claim to be other vehicles since they only interact with their anonymous public keys vehicles cannot cheat about their position and related parameters if a secure positioning solution is used a vehicle cannot deny having sent a message because it is signed by an anonymous key that belongs exclusively to the sender. Using these facts, the security of a VANET is more a certainty than an assumption. Yet, many problems can occur when trying to solve the basic issues of security in IVC. In order to preserve the driver's anonymity and minimize the storage costs of public keys, a key changing algorithm that adapts to the vehicle speed can be propose. Also the algorithm takes into account key correlation by the attacker. On one hand the anonymous key set size should be small to reduce storage space on vehicles, but also on the other hand the certificate lifetime should be short to reduce the vulnerability window of the system if an anonymous public or private key is compromised. Therefore, a tradeoff must be made between the two. The life time certificate uses the following aspects: each anonymous key should be used only with a sequence of consecutive messages. Also, the lifetime certificate should be short, around one day, to limit in the effects of a possible key compromise. On the other hand, driving duration changes from day to day, hence some days a larger number of keys may be required. To account for this, the lifetime certificate should be stretched over several days. Another important aspect that has to be taken in consideration is that a vehicle should change its anonymous key only after having used it for a certain number of messages. As we propose using a PKI for supporting security in VANETs, it is important to choose a Public Key Cryptosystem (PCKS) with an acceptable duration overhead in vehicular context like the following: RSA sign: the key and signature sizes are large (256 bytes).

ECC (Elliptic Curve Cryptography): it is more compact that RSA (28 bytes), faster in signing but slower in verification. NTRU Sign (a recent cryptosystem) the key size is of approximately 197 bytes, but it is much faster than both in both signing and verification.

4 Conclusion

The security of VANET of the road condition information transferring system is crucial. For example, it is essential to make sure that life-critical information cannot be inserted or modified by an attacker. The system should be able to help establish the liability of drivers; but at the same time, it should protect as far as possible the privacy of the drivers and passengers. In fact, there are very few academic publications describing the security architecture of VANETs. So integrate the characteristics of ad hoc network itself, in the ITS of this paper, we concern the security issues of VANETs from only a few aspects based on some referential papers and provide the appropriate solving measures.

References

[1] G. Samara, *et al.*, "Security issues and challenges of Vehicular Ad Hoc Networks (VANET)," in *4th International Conference on New Trends in Information Science and Service Science (NISS)*, 2010, pp. 393-398.

[2] B. K. Chaurasia, *et al.*, "Attacks on Anonymity in VANET," in *International Conference on Computational Intelligence and Communication Networks (CICN)*, 2011, pp. 217-221.

[3] G. Samara, *et al.*, "Security Analysis of Vehicular Ad Hoc Networks (VANET)," in *Second International Conference on Network Applications Protocols and Services (NETAPPS)*, 2010, pp. 55-60

[4] M. Burmester, *et al.*, "Strengthening Privacy Protection in VANETs," in *IEEE International Conference on Wireless and Mobile Computing Networking and Communications, WIMOB '08.*, 2008, pp. 508-513.

[5] Chim, TW, Yiu, SM, "SPECS: Secure and Privacy Enhancing Communications Schemes for VANETs," Ad Hoc Networks, Volume 9, Issue 2, March 2011, pp. 189-203.

[6] F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, E. Schoch, B. Wiedersheim, Ta-Vinh Thong, G. Calandriello, A. Held, A. Kung, J.-P. Hubaux, Secure vehicular communication systems: implementation, performance, and research challenges, IEEE Communications Magazine, vol. 46, no. 11, pp. 110-118, November 2008

[7] S. Tsugawa, "Issues and Recent Trends in Vehicle Safety Communications Systems" IATSS Research, Vol.29, No.1pp.7-15(2005.2)

[8] P. Golle, D. Greene, “Detecting and Correcting Malicious Data in VANETs”. In Proceedings of the First ACM Workshop on Vehicular Ad Hoc Networks, pp. 29-37, 2004.

[9] N. Sastry, U. Shankar and D. Wagner. “Secure Verification of Location Claims”. In ACM Workshop on Wireless Security. WiSe 2003.

[10] M. Raya, P. Papadimitratos, and J.-P. Hubaux, Securing Vehicular Communications, In IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, October 2006

[11] M. Raya and J.-P. Hubaux, Security Aspects of Inter-Vehicle Communications, *In Proceedings of STRC 2005 (Swiss Transport Research Conference)*, March 2005

[12] P. Papadimitratos, V. Gligor, and J.-P. Hubaux. Securing Vehicular Communications - Assumptions, Requirements, and Principles, In Proceedings of the Workshop on Embedded Security in Cars (ESCAR) 2006, November 2006.

[13] V. Paruchuri, "Inter-vehicular communications: Security and reliability issues," in *International Conference on ICT Convergence (ICTC),* , 2011, pp. 737-741.

[14] A. Wasef*, et al.*, "Complementing public key infrastructure to secure vehicular ad hoc networks [Security and Privacy in Emerging Wireless Networks]," *IEEE Wireless Communications,* vol. 17, pp. 22-28, 2010.

[15] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, J.-P. Hubaux, Secure vehicular communications: design and architecture, IEEE Communications Magazine, vol. 46, no. 11, pp. 100-109, November 2008

[16] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, Mix-Zones for Location Privacy in Vehicular Networks, In Proceedings of WiN-ITS, August 2007