Analysing Security Threats and Defensive Strategies Along with Misbehavior Detection in VANETS

Needra Fernando[1] Maheswari Mangai[2] Senthil Kumaar[3], Prabu[4]
[1, 2, 3]PG Scholar, [4]Asst Professor
[1, 2, 3]Department of Information Technology
[1, 2, 3]Veltech Multitech Engineering College, India

Abstract---Vehicular Adhoc Networks (VANET) are becoming more popular as the need for accessing and sharing data while on the move is increasing. Value-added applications such as online payment services, geographical location identification, etc. in VANET, improve driving safety, passenger comfort, offer great business opportunities, and attract more and more attention in our daily life. VANETs connect vehicles into a huge mobile adhoc network to share information on a larger scale. The various attacks in VANETs are the Sybil attack, DDOS attack, misbehaving and faulty nodes, sinkhole attack, spoofing, traffic analysis attack, position attack, and illusion attack. Providing security to VANET is important in terms of providing user anonymity, authentication, integrity, and privacy of data. In this paper, a comprehensive survey on the threats and vulnerabilities in VANETs are explored and analysed in detail. The compromised security goals are identified for each threat. The existing solutions for these threats are discussed in this paper.

Keywords: VANET, Security, Adhoc, Attacks in VANETs

I. INTRODUCTION

A Vehicular Adhoc network (VANET), a form of Mobile Adhoc Networks (MANETs), provides communication among nearby vehicles, between vehicles, and nearby fixed equipments called Road Side Units (RSUs). Fig. 1 shows the VANET architecture. Every node i.e., a vehicle or RSU communicates with other nodes in single hop or multi hop. VANETs are designed with the goals of enhancing driving safety and providing passenger comfort. In VANETs, the types of communication are the following:

- Vehicle-to-Vehicular (V-V) or Inter-Vehicular Communication
- Vehicle-to-Infrastructure (V-I) or Vehicle-to-Roadside Communication
- Inter Roadside Communication.

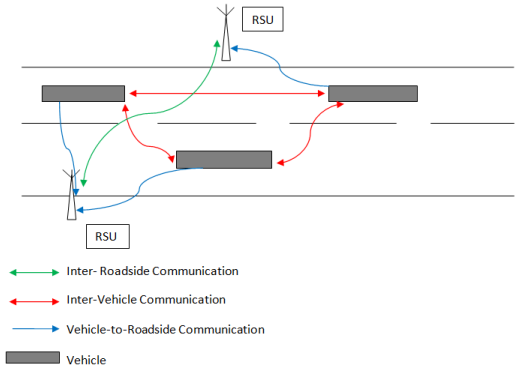

Fig. 1: VANET Architecture

The radio used for the communication is Dedicated Short-Range Communications (DSRC). DSRC/WAVE is part of the Federal Highway Authority's Vehicle Infrastructure Integration (VII) initiative and supports vehicle-to-vehicle (V-V) and vehicle-to-infrastructure(V-I) communications for emerging Intelligent Transportation Systems (ITS). DSRC/WAVE systems remove the drawbacks in the wireless infrastructure by aiding low latency, geographically local, high data rate, and high mobility communications [1]. This includes data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure in the licensed ITS band of 5.9 GHz (5.85-5.925 GHz). IEEE 1609 is a higher layer standard based on the IEEE 802.11p. The characteristics of VANETs are as follows:

- High mobility with the constraint of road topology
- Potentially unbounded network size
- Time-sensitive data transfer
- Accurate positioning access (GPS)
- No power issues
- Deployment in direction of roadway
- Large scale connection range and large number of nodes

The security of VANETs is a critical issue because the information transmission is in wireless environment. Itconstitutes short-range radios installed in vehicles, Road Side Units (RSUs), and central authorities which are responsiblefor identity registration and management. VANET projects have been used by various industries, governments, andacademic institutions around the world these years. But VANETs are susceptible to intruders ranging from passiveeavesdropping attack to active spamming, tampering, and interfering due to the absence of basic infrastructure andcentralized administration.

VANETs do not have very high power source, fixed infrastructure, and continuous connectivity. Also, there is nofixed route between mobile nodes as they join/leave networks. Thus, vehicular communication is inherently vulnerable tomany threats. VANET communication is completely wireless technologies viz. Wi-Fi, DSRC. Any intelligent nodewithin the transmission range of a sender node can potentially receive the message over the same wireless link. Thisoften leads to passive attack (eavesdropping, traffic analysis), active attack (replay attack), or a combination of both.

Wireless environment makes it difficult to differentiate between malicious behaviour and real-life behaviour. Amalicious node can purposefully drop or discard packets. Similar kind of behaviour can be experienced in a wirelessnetwork because of limited bandwidth, weak links, and the mobility of nodes.Routing in VANET has also vulnerabilities. Routing in VANET can be unicast, multicast, geocast, mobicast, orbroadcast [2]. The unicast routing protocols are classified into min-delay and delay-bound approaches. The min-delayunicast routing

protocols construct a minimum-delay routing path in least time. The delay-bound routing protocol makesuse of the carry-and-forward technique to reduce the channel utilization within a constrained delay time.

The multicast inVANETs deliver multicast packets from a mobile vehicle to all multicast-member vehicles. The geocast routing geocastpackets from a source vehicle to vehicles located in a specific geographic region are delivered. Mobicast routing protocolin VANETs is also present. An intermediate node can advertise ¢wleast-cost-path¡ü to a certain destination to intercept intothe traffic for that node. Intermediate malicious nodes may drop packets intentionally. For table-based routing systems,malicious nodes may provide false information to jeopardize the routing tables of other nodes. A security system has tobe ensured so that transmission comes from a trusted source and is not tampered en-route by other sources.

The following part of this paper is organized as follows. Section 2 explains the importance of providing security inVANETs. Section 3 deals with the security breaches possible in VANETs, the security goals compromised by thesebreaches, and the vulnerabilities. Section 4 describes the existing methods to prevent and identify these attacks. Section 5 deals with misbehavior detection and section 7 concludes the paper.

II. MOTIVATION

In applications like online transactions, banking, etc., secrecy of data has to be maintained. With the increasingnumber of applications in VANETs, the various types of attacks on VANETs are also increasing. Due to these attacks,data confidentiality is threatened, life of the passenger may be at risk, and services may be denied to the authenticatedusers. Hence, importance has to be given to secure these networks from malicious users that threaten the security goals.Our motivation is to provide a real time solution to prevent the attacks in VANET.

III. SECURITY GOALS

The goals to secure VANETs are the same as that for securing any network. The main objective is to provideauthentication, confidentiality, integrity, availability, and non-repudiation.

Authentication is the assurance that the communicating entity is the one that it claims to be. It enables a node toconfirm the identity of the communicating node. It is also important that the node receiving the data is sure thatthe data is sent from a valid sender. For eg. The vehicles transmitting should be an authenticated user registeredto a Certificate Authority in order to uniquely identify the vehicle.

1) Authentication is the assurance that the communicating entity is the one that it claims to be. It enables a node toconfirm the identity of the communicating node. It is also important that the node receiving the data is sure thatthe data is sent from a valid sender. For eg. The vehicles transmitting should be an authenticated user registeredto a Certificate Authority in order to uniquely identify the vehicle.
2) Confidentiality deals with the protection of data from unauthorized disclosure. Confidentiality of data ensuresthat the data is not leaked or disclosed to unauthorized nodes. Disclosure of this data may lead to identificationof vital information. For eg. The data being transmitted by the vehicles should be received by the registeredvehicles only.
3) Integrity is the assurance that the data received are exactly the same sent by the authorised node without anymodification, deletion, insertion or replay. To ensure integrity of data unauthorised manipulation must bedetected. For eg. The content of the messages sent between the vehicles should not be changed.
4) Availability assures that the system works properly and that service is provided to authorised users as and when required. An adversary may deny services to valid nodes by jamming the channel, by disrupting the routing protocol, by draining the battery power, etc. For eg. The services provided by the RSU should be available to the vehicles whenever it is required.
5) Non-repudiation provides protection against denial by one of the entities involved in a communication of being participated in all or part of the communication. For eg. After sending a message, the vehicle should not deny having sent the message. This is called sender non-repudiation. Also after receiving a message, the vehicle should not deny having received the message. This is called receiver non-repudiation.

IV. ATTACKS IN VANET

In this section, the threats and vulnerabilities in VANETs are discussed.

A. A.bruteforce attacks on keys

Key management deals with the secure generation, distribution and storage of keys. For ad hoc networks, the current literature reports three main approaches for key management: key exchange, key agreement and key management infrastructure. The distribution of safety-related information (such as turn warnings, speed limit information, etc.) is a major application of VANET. In VANET communication, keys are used for encrypting data. Brute force attack is an exhaustive key search strategy by checking all possible key values [3]. If the confidentiality of the keys is lost, the identity of the vehicle is lost. Integrity and authenticity of the node is also compromised.

B. Traffic analysis attack

Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. Traffic data comprises the time and duration of a communication, the detailed shape of the communication streams, the identities of the parties communicating, and their location. Techniques to prevent traffic analysis attacks on the internet have been an active area of research as well. Depending on the communication patterns, the type of information in the observed communication can be understood.

C. Sybil attack

Sybil attack is a kind of impersonation, where multiple identities of the attacker node are present. With several entities in the network it will be able to reduce the effectiveness of fault-tolerant schemes. Fig. 2 shows the

Sybil nodes assuming multiple personalities of the attacker node.

- In Sybil attack, a malicious node fabricates different identities in the form of multiple nodes.
- These fabrications mislead neighbouring vehicles by communicating with other physical nodes and distributing false traffic information (e.g., traffic jam or accidents).
- This attack is very dangerous in geographical routing because a node can claim to be in several positions at the same time.

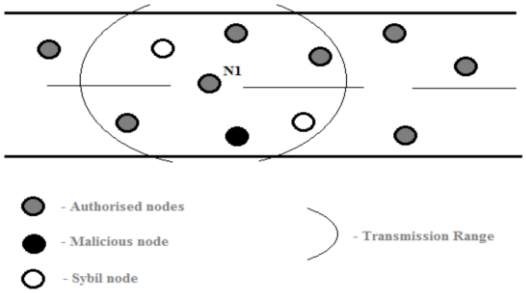

Fig. 2: Sybil Attack

Sybil attacks can incur great security threats to VANETs. First, Sybil nodes may cause an illusion of traffic congestion. A greedy driver may convince the neighbouring vehicles that there is considerable congestion ahead, so that they will choose alternate routes and allow the greedy driver a clear path to his/her destination. Second, Sybil nodes may directly or indirectly inject false data into the networks, greatly impacting on the data consistency of the system [4]. For example, VANETs may rely on multiple vehicles voting to generate a traffic status report. However, if some of the voters are Sybil vehicles, the report may be deviated from the fact, depending on the benefits of the malicious. Finally, Sybil nodes may launch further DoS attacks such as channel jamming attacks and message suppression attacks. D. DENIAL OF SERVICE (DoS)

In DoS attack the main objective is to prevent the legitimate user from accessing the services and from the resources [5]. The attack occurs by jamming the network or channelling the system so that no vehicle can access it. This avoidscommunication completely in the network which is devastating in real time applications. Example attacks include channel jamming and aggressive injection of dummy messages. Three different ways in which the attacker can achieve this are [5]:

a. In basic level, the attacker overwhelms the node resource so that the node becomes continuously busy and will not be able to process further as shown in Fig.3.

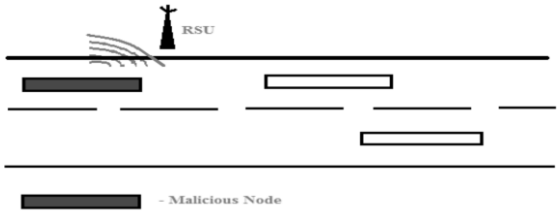

Fig.3: Attacker overwhelms node resources

b. In extended level, the attacker jams the channel by generating high frequency in the channel as shown in Fig. 4. Thus the vehicle will not be able to communicate in the network.

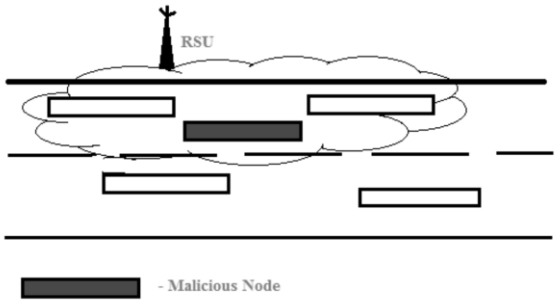

Fig. 4: Jamming the channel

D. Sinkhole attack

In sinkhole attacks, all the traffic from a particular area goes through the attacker node. Therefore, the attacker will have control over the traffic, enabling the occurrence of many other attacks, such as selective forwarding. Fig. 5 shows the malicious node transferring the data to the sink node. Wormhole attacks can be considered as a subclass of sinkhole attacks, where two nodes create a tunnel between them and forward the packets through it. This can be useful to lure a node of a better path to the destination.

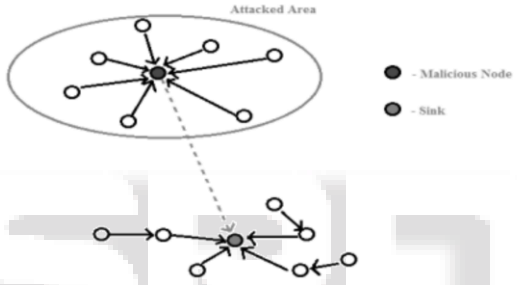

Fig. 5: Sinkhole Attack

E. Selective forwarding

In selective forwarding specific packets are always dropped. As dropping all packets can be easily detected by neighbours, the attacker performs a selection on the packets. Thus attacker forwards some of the messages, being able to degrade the service anyways [3].

F. Misbehaving and faulty nodes

Vehicular network (VN) nodes (road-side infrastructure units and vehicles) that participate in network operations has a certificate issued by a Certification Authority (CA). But the possession of a certificate does not assure correct information from the node: a node may inject false data (e.g. alerts, warnings, coordinates) while adhering with the implemented protocols [3]. The eviction of misbehaving nodes can be achieved by revocation of a node's certificates. Therefore messages from this node will not be valid after the certificate revocation. However, the absence of an omnipresent roadside infrastructure, mainly in the early deployment stages, and the large-scale deployment of VANETs prevent the application of traditional certificate revocation schemes. Also, unless a node is revoked for administrative reasons (e.g. the vehicle owner did not renew its registration), it becomes difficult for the authority to obtain and validate sufficient evidence that a node is faulty or compromised. Thus, an additional challenge is the protection of non-misbehaving nodes until they obtain the revocation information regarding misbehaving nodes.

G. Illusion attack

Illusion attack is a new security threat on VANET applications where the adversary intentionally deceives sensors on her/his own vehicle to produce wrong sensor readings [6]. As a result, the corresponding system reaction is invoked and incorrect traffic warning messages are broadcasted to neighbours, creating an illusion condition on VANET. An attacker must create a virtual traffic event to produce an illusion attack. Two prerequisite conditions must be achieved by the attacker to create the virtual traffic event. The first condition is to realise or create the prerequisite traffic situation on the road. Second, the false traffic warning messages should be generated and distributed by the attacker. The traditional message authentication and integrity check used in wireless networks are inadequate against the illusion attack. Fig. 6 shows how the concept of Illusion attack is brought in VANETs.

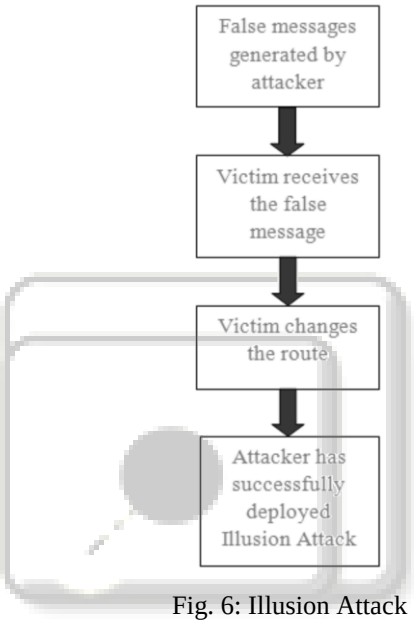

Fig. 6: Illusion Attack

H. Position attacks

Location refers to vehicle position in a VANET. It is one of the most valuable information (used in geographic routing) and is often readily available through positioning services such as global positioning system (GPS). Position attacks occur when the line of sight of radars is blocked. An attacker launches a position attack by modifying position packets, replaying bogus position packets, and dropping urgent position packets. Position cheating and false position disseminating: VANETs have special requirements in terms of node mobility and position-dependent applications. These requirements are adequately met by geographic routing protocols.

Wrong position information is due to malfunction in the positioning hardware or falsified intentionally by attackers to reroute data. Malfunctioning nodes may degrade the performance of a system to some extent while rerouting of data through malicious nodes violates basic security goals such as confidentiality, authenticity, integrity, and accountability. The attacks can be classified as passive attacks, active attacks, and insider attacks. A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks.

I. Exisiting detection mechanisms for attacks in vanets

A secure authentication method uses a unique identification for vehicles concatenated with some large random value to prevent Brute force attack. These concatenated values are then hashed using hash algorithm proposed in [8]. To deal with traffic analysis attack, VIPER: a vehicle-to infrastructure communication privacy enforcement protocol is proposed in [9]. In this, vehicle will not send their messages directly to RSU but randomly uses neighbouring vehicles as intermediates. In [10], a novel solution is proposed to detect Sybil attack. In the proposed solution, the Sybil identities of the node are observed by its neighbours for a fixed time and the data from the neighbouring nodes are compared. If a set of nodes are simultaneously observed by neighbouring nodes for a duration greater than threshold value, then these set of nodes are grouped under Sybil group category. DoS attack solution is based on the use of On Board Unit (OBU) that is installed in vehicles. The OBU has a supporting processing unit that tells the OBU to switch channel, technology, or to use frequency hopping technique or multiple transceiver [11]. Misbehaving and Faulty nodes are identified by using a CA and a protocol for eviction of attacker and a local detection for individual misbehaviour of node [12]. Illusion attack can be identified by a Plausibility Validation Network which helps to validate the messages that are received at a vehicle [6]. Position Attacks can be prevented by the Autonomous Position Verification method in which a node does not use hardware used in the network to verify the position claimed by the node [3].

J. Misbehaviour detection

VANETs and other CPSs share a number of characteristicsthat require fundamentally new approaches forsecurity, which differ from existing IT security requirements.

a. Critical usage scenarios.

CPSs often control systemswhere failure or malfunction may have severeconsequences, including massive financial loss orloss of lives. Often, these systems fall under theterm critical infrastructures (CI). VANETs are oneexample where failure or malfunction may leadto massive congestion with subsequent delays andfinancial losses or even to accidents with loss oflives in a worst case.

b. No clear security perimeter.

In many of thesesystems, there is no clear boundary between insidersand outsiders. Instead, the logically and physicallydistributed nature of CPSs leads to unclear securityperimeters and possible insider attacks. VANETsare again a core example, as such networks are cooperativelyformed by vehicles and road-side equipment.As vehicles are under distributed ownershipand control, it needs to be assumed that some ofthe vehicles are under full control of attackers.

c. Limited physical security.

As nodes in CPSs areoften distributed in a potentially hostile environment,they may be subject to hijacking, analysis,and reprogramming by attackers. Due to cost constraints,the protection against such hijacking isoften limited. A typical example is a Wireless SensorNetwork for environmental monitoring, wherenodes may be scattered randomly in the environment.Due to the long lifetime of vehicles,

similarchallenges can be found in both VANETs and invehiclenetworks.

d. Sensor values as security assets.

The primarysecurity assets in CPS are the sensor values and theactuators controlled based on this input. Spoofingand manipulation of sensor data are thus primaryattack vectors. For instance, in a VANET that isused for detecting traffic jams, an attacker maywant to suppress certain sensor readings that wouldindicate a traffic jam, or inject sensor values thatindicate a traffic jam where none exists.In summary, CPSs, and VANETs in particular, willlikely attract attackers that try to manipulate sensed dataand influence the resulting actions taken by the system.

Such attackers may participate as regular network entitieseither because attackers can easily join the VANET orhijack already participating nodes. Once an attacker hasentered the VANET, she can easily inject spoofed information into the VANET and trigger incorrect behavior.From the perspective of the VANET, this attacker can beseen as a misbehaving node that is sending incorrect data.

In addition to information injection and manipulation,other attack types are conceivable, such as compromisingrouting efficiency by not forwarding information forother nodes. In this paper, we focus on detection ofinformation manipulation. Note we cannot necessarilydistinguish whether information manipulation is due tomalicious intent or due to faulty hardware.

However,from an information quality perspective, the resultingcountermeasures should arguably often be the same.Classical IT security mechanisms, like encryption,signatures, access control, (signature-based) intrusiondetection systems, and so forth, are not suitable tothwart such insider attacks. Instead, we need securitymechanisms that can identify misbehavior, identify themisbehaving node, and react either by filtering out theincorrect data or excluding the misbehaving node fromfurther participation in the VANET. Research on securityin VANETs has already developed several novel ideas forthese tasks, many of which align with the goals of otherCPSs.

Node-centric mechanisms require authenticationmechanisms to reliably distinguish between differentnodes. Many systems achieve this by assuming a trustedthird party like a PKI that issues credentials, whichare then used to authenticate messages and the correspondinginformation, using a security mechanism likedigital signatures. Node-centric mechanisms can furtherbe divided into behavioral and trust-based mechanisms.

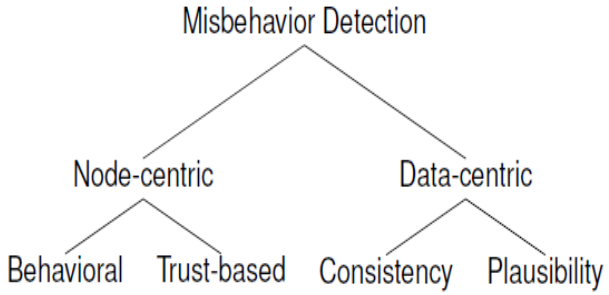

Fig. 7: Taxonomy of misbehavior detection

On the other hand, trust-based mechanisms inspect thepast and present behavior of a node and use this to derivea probability for future misbehavior. The assumption isthat a node who behaved correctly in the past is morelikely to behave correctly in the future. Essentially, thisboils down to some form of reputation managementscheme where correct behavior increases the reputationwhile misbehavior reduces it. These mechanisms are
commonly used for reporting and local revocation of
nodes in a VANET, for example through LEAVE [10].

Finally, plausibility checking mechanisms are allmechanisms that have some implicit or explicit model ofthe real world and check whether incoming informationis plausible within this model. For instance, in VANETs,speed reports of 700 km/h are not very plausible and maybe filtered out. However, plausibility should be appliedwith caution in VANETs, as part of the focus of suchnetworks is to detect outliers that indicate important, butrare, events, such as collisions between vehicles.

V. CONCLUSION

Safety and security is becoming a necessity for VANET applications. As VANETs use wireless technology, it is vulnerable to many attacks. In this paper, the attacks in VANETs, the security goals compromised by these attacks, and their prevention/detection mechanisms have been discussed. Among these attacks Illusion Attack is a serious threat that assists an attacker to hijack a car or to have a clean getaway after a theft or robbery. Our future work is to propose a solution to detect Illusion attack.

REFERENCES

[1] IEEE Standard for Information Technology – Telecommunication and Information exchange between Systems – Local and Metropolitan Area Networks – Specific Requirements, IEEE Std 802.11p™ - 2010

[2] Yun-Wei Lin, Yuh-Shyan Chen and Sing-Ling Lee, ―Routing Protocols in Vehicular Ad Hoc Networks: A Survey and Future Perspectives‖, Journal Of Information Science And Engineering 26, 2010, pp 913-932

[3] J.T. Isaac, S. Zeadally, J.S. Ca´Mara, ―Security Attacks And Solutions For Vehicular Ad Hoc Networks, IET Communication‖., 2010, Vol. 4, Iss. 7, Pp. 894– 903.

[4] Bin Xiao, Bo Yu, ChuanshanGao, ―Detection And Localization Of Sybil Nodes In VANETs‖, Diwans'06, September 26, 2006.

[5] HalabiHasbullah, 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 65 2010

[6] Nai-Wei Lo, Hsiao-Chien Tsai, ―Illusion Attack On VANET Applications – A Message Plausibility Problem‖, Global Workshops, IEEE 2007

[7] Leinmu¨ Ller T., Maiho ¨ Fer C., Schoch E., Kargl F.: ―Improved Security In Geographic Ad Hoc Routing Through Autonomous Position Verification‖. Third Int. Workshop On Vehicular Ad Hoc Networks (VANET 2006), 2006, pp. 57–66

[8] Langley C., Lucas R., Fu H.: ―Key Management In Vehicular Ad-Hoc Networks‖. IEEE Int. Conf. on Electro/Information Technology (EIT 2008), 2008, pp. 223–226
[9] Cencioni P., Di Pietro R., ―A Mechanism To Enforce Privacy In Vehicle-To-Infrastructure Communication‖, (2008) Computer. Commun (12), pp. 2790–2802.
[10] Jyoti Grover, Manoj Singh Gaur, Vijay Laxmi, Nitesh Kumar P, ―A Sybil Attack Detection Approach using Neighbouring Vehicles in VANET‖,ACM, Sydney, 2011
[11] I.AhmedSoomro, Hbhasbullah,J.Lb.AbManan,‖Denial Of Service (Dos) Attack And Its Possible Solutions In VANET ‖, Waset Issue 65, April 2010 Issn 2070-3724.
[12] Raya M., Papadimitratos P., Aad I., Jungels D., Hubaux J.: ―Eviction Of Misbehaving And Faulty Nodes In Vehicular Networks‖, IEEE J. Sel. Areas Commun., 2007, 25, (8), pp. 1557–1568.

