A Survey on Sybil Attack in Vehicular Ad-hoc Network

Deepak Kushwaha
PG Student
Department of CSE
UIT RGPV, Bhopal, India

Piyush Kumar Shukla,
Ph.D
Assistant Professor
Department of CSE
UIT, RGPV, Bhopal, India

Raju Baraskar
Assistant Professor
Department of CSE
UIT, RGPV, Bhopal, India

ABSTRACT
Vehicular Ad-hoc network is new and emerging technology. Researchers are gaining interest in this technology. Due to its open nature it is vulnerable to various attacks. Sybil attack is one of them. Various defense techniques have been given by researchers. In this work we briefly explain those defense techniques, given recently. We categorize these techniques as trusted certificates base, resource testing based and social network based. We give an overview of some defense schemes based on first two categories. We also give a summary of the techniques given in this paper, which is based on some parameters used in those techniques.

Keywords
Vehicular Ad-hoc Network, Sybil Attack, Certification Authority.

1. INTRODUCTION
For past two decade vehicles were not only realm of mechanical engineers but gaining interest of computer engineers also. Now next generation vehicles would have equipped with some kind of hardware named On Board Unit (OBU) that allows them to communicate with other vehicles as well as roadside-units and they form a communication network that we call vehicular ad-hoc network (VANET). The main aim of VANET is to make roads safer and efficient by providing timely information to the other drivers and concerned authorities this is called as Intelligent Transportation System (ITS). Development of such type of networks has bought number of security issues those are related to mobile and wireless communication and user privacy. Because of the open nature of VANET they are vulnerable to various types of attacks. Attackers also categorizes as inside attacker and outside attacker. Some of the attacks which may impair VANET are as follows

1.1 Types of Attacks

1.1.1 Denial of Service attack
This type of attack can be carried out by network insider or outsider. In this attack an attacker can block network for authentic users by flooding or jamming the signal.

1.1.2 Spamming
If there are spam messages in VANET then they may elevate the risk of increased transmission latency. As VANET lacks the presence of some basic infrastructure and centralized administration spamming is very difficult to control.

1.1.3 Black Hole Attack
If a node drops all the messages coming to it for routing purpose is called as black hole attack or we can say that when a node refused to participate in the network is called as black hole attack.

1.1.4 Replay Attack
In replay attack an attacker repeatedly injects data into network to degrade the performance of the network.

1.1.5 GPS Spoofing
It is a type of attack in which a malicious driver uses a Global Positioning System (GPS) satellite simulator to generate stronger signals than those generated by genuine satellite. By using this GPS simulator an attack can make fool other drivers that they are in a different location by providing false reading in victim's GPS device.

1.1.6 Position Faking
Unsecure communication in VANET can allow an attacker to modify its actual position to another position and pass it to other vehicles. In this way he is broadcasting its fake position which may cause damage to many lives.

1.1.7 Message Tampering
It is a threat to authenticity. If an unauthorized user is able to modify the messages exchanged during vehicle-to-vehicle or vehicle-to-infrastructure communication then he/she may inject false information in the network which may cause damage to many lives.

1.1.8 Broadcast Tampering
This type of attack is performed by an insider attacker in which an attacker injects false messages in the network to cause damage.

1.1.9 Malware
It is a type of attack in which a virus or worm is entered into the VANET and make communication very slow by eating resources. Virus and worms may enter in VANET during software or firmware upgrade in OBU and RSU or an insider attack may manually inject virus or worm in the OBU or RSU.

1.1.10 Sybil Attack
It is type of attack in which a malicious driver creates multiple fake identities to make illusion that there is very heavy traffic nearby him so the traffic following him may choose alternate route and attacker would get empty route for himself.

These are some attack that may be performed in a VANET environment by an attacker. Various solutions have been given by authors for these attacks. In this paper we shall consider only Sybil attack in detail. We briefly describe some of the schemes to detect Sybil attack in VANET and describe the comparative study of these detection schemes.

Sybil attack is a very critical security issue in vehicular ad-hoc network. Sybil attack was first introduced by Douceur [11] in peer-to-peer networks. Authors have given various methods to detect Sybil attack. In Sybil attack one malicious vehicle have control over other Sybil nodes and may have control over other networking protocols also. For example in presence of Sybil nodes result of some voting based protocols may be deviated and Sybil nodes may also launch Denial of Service attack to impair the normal operations of data dissemination protocols [13, 14, 15]. Sybil attack can be detected by using three types of techniques [12] a) Radio resource testing, based on an assumption that a radio cannot send or receive simultaneously on the same channel. b) Identity registration, based on that each vehicle should have a unique identity as issued by some centralized authority. c) Position verification, based on the malicious node create some fake identities at different position so on the basis of the physical position of the node.

Some authors propose schemes that are centralized in nature and some propose schemes those are not centralized in nature. Schemes those are centralized in nature have a centralized trusted authority and that authority issues some form of certificate unique for each vehicles but the schemes those are not centralized in nature use other form of techniques to detect Sybil attack for example resource testing or position verification etc. Mekliche et el [8] proposed a scheme that is centralized in nature i.e. there is centralized authority authors call it Department of Motor Vehicle (DMV) , they may issue a pool of pseudonyms for vehicles, by which a vehicle can be uniquely identified but this identity can be made hidden so that vehicles' privacy can be preserved. Authors also use support of RSU which authors consider a semi trusted unit. Some authors also gave social based Sybil attack defense. So in this way we can categorize Sybil defenses in three categories. As shown in fig 1.

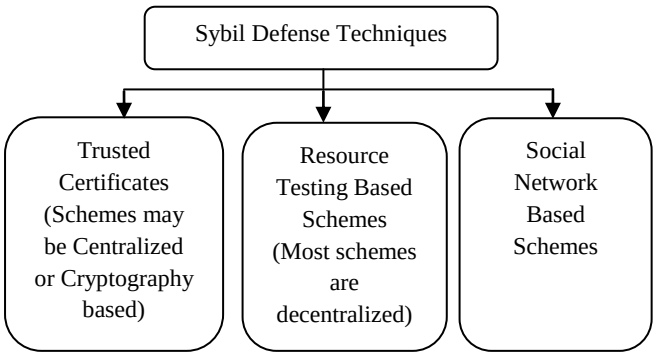

Fig 1: Categorization of Sybil Defense Techniques

Chang et al. [3] gave a throughout survey of Sybil attack in networks in which authors summarized some existing defense techniques till that time and gave idea for research in that area. In their work authors categorize defense techniques by their designed time. In this survey authors categorize various types of attackers and then categorize the Sybil defense techniques. Authors also pointed out the problem in those defense techniques. Authors not only categorize the techniques to defend Sybil attack but also gave work proposed by authors till date.

The rest of this paper is organized as follows. In section II we give survey of recent work to detect Sybil attack. In section III we summarize all the survey done in section II using some key characteristics. And in section IV we conclude our work.

2. SURVEY ON SYBIL ATTACK

Bo Yu et al. [5] presented an integrated scheme to detect Sybil attack in vehicular ad-hoc network. In that detection method they use 1) cooperative detection method in which each node cooperates to detect Sybil node. In this cooperative detection method each node periodically perform three roles a) claimer b) witness c) verifier after performing verification from the verifier, the node is able to detect a Sybil node. In cooperative detection method they estimate the position of the node using Received Signal Strength (RSS).This method did not work well because if witness itself is a Sybil node then result may not be accurate. To overcome this problem they consider that the vehicles coming from opposite direction may be trusty witness, to identify traffic of opposite direction they give 2) presence evidence system for identification of vehicles going on opposite lane, they make use of RSU deployed at uniform distance along the road. When a vehicle passed by an RSU, it issue a position certificate to the vehicle which consists position of RSU with time stamp. When this vehicle encounter with another vehicle on the way they exchange the position certificate and a verifier node can identify a vehicle that it is on the other lane of the road. So by this way verifier can identify traffic which is coming by opposite lane and witnesses are taken from that lane only. Authors in this article integrate the schemes 1 and 2 to detect Sybil nodes in the network; they use statistical detection method to detect Sybil nodes which is based on the radio propagation model.

Hussain et al. [9] presented a scheme in which they detect not only Sybil attack but also privacy is preserved of a node. In this scheme pseudonym-less beaconing is used to preserve privacy of node and for Sybil attack detection a temper resistant module is used to carry out pre-assembly analysis of data, this data is used to assemble beacons. Authors introduced a new term called as Event Reporting Message (ERM). ERMs are supported by RSU to get suspected Sybil nodes in its range and RSU report those nodes to revocation authority. In this scheme RSUs distribute authorized tokens to benign vehicles and by using those tokens node report ERMs. RSUs collect those ERMs for particular event and checks if, more than one ERMs contain the identical token. If RSU found such type of ERMs, it reports those ERMs to revocation authority. In turn revocation authority takes particular action against those nodes.

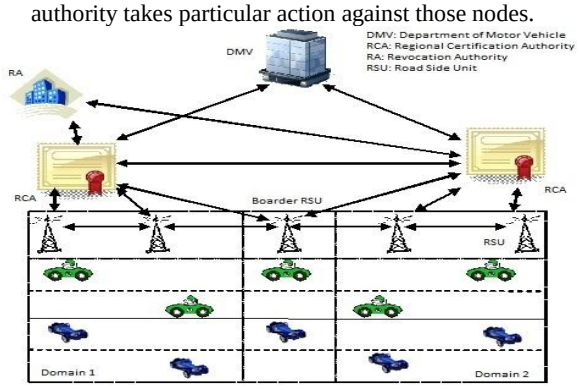

Fig 2: Network Model of [9]

The network model given in [9] is a good model in which there is centralized trusted authority which is department of motor vehicles (DMV) at the top of the hierarchy, its responsibility is to initialize and generate registration of the vehicles and road-side infrastructure. Below it there are some

revocation authorities (RA) and regional certification authorities those are considered as semi-trusted authorities. Main function of revocation authority is to take a particular action when a Sybil node is detected by the road-side unit and RCAs are responsible for generating certificates for road-side units. In the hierarchy RSUs comes next to RAs and RCAs, main function of a RSUs is to generate tokens to each vehicles in the vicinity and detect unfamiliar behavior of vehicles, if a vehicle is detected malicious then RSU report that vehicle to RA to take particular action. All the vehicles reside at the bottom of the hierarchy.

Bayrem et al. [1] proposed a RFID based solution for detecting Sybil attack in VANETs. In this paper they assume that the network is divided into several zones, in each zone there are several RSUs and one of those RSU is selected as the controller of that zone called as road side controller (RSC). Every RSC is attached to a central certification authority and when vehicles moves from a zone to different zone, vehicles are required to change their certificates. Two types of authentication techniques are used to detect Sybil attack. In first technique they consider that every vehicle embedded with active RFID tags to securely authenticate every vehicle by RSU and obtain short lifetime certificates. Second technique is based on the use of those short lifetime certificates by vehicles to be authenticated by neighboring vehicles. This technique allows detection of Sybil attack in or out of range of RSU; this is because an observer component is deployed in vehicle. Every RSU is equipped with tamper-proof RFID reader to read RFID tag of vehicles. As the vehicle enters in a new zone RFID tag reader reads the RFID of vehicle and authenticate each vehicle by data extracted by database which is attached to reader. Privacy of vehicle is another issue to resolve this issue a lightweight privacy preserving authentication protocol can be used. EPCglobal class-1 Gen-2 RFID system [16] is suggested by authors. A 32-bit pseudo random number is generated at RFID tag to hide electronic product code (EPC). A Sybil attack may be that an attacker can use certificate belongs to another zone, this type of attack can be detected as when neighboring vehicles receive broadcast message by attacker, it can be authenticated using certificates of another zone and can easily identified that it is using fake identity. Neighboring vehicle send a report that contain temporal identity of vehicle with timestamp of event to RSU. Some other type of Sybil attack can also be detected in this work.

Zhou et al. [10] gave a Sybil attack detection scheme for VANET named P^2DAP. In this scheme they assume department of motor vehicle (DMV) as a trusted entity, road side unit (RSU) as a semi trusted entity and vehicles are not considered as trusted entity. DMV maintains vehicle records and issue pseudonyms to the vehicles. In this paper authors gave a privacy preserved solution "P2DAP" to detect Sybil attack. Privacy of a vehicle is preserved by pseudonyms issued by DMV; and those pseudonyms are also used by vehicular nodes to communicate in secure manner. The problem could be that an attacker can use multiple pseudonyms to pretend to be multiple vehicles. To overcome this problem authors of "P2DAP" generate pseudonyms for a particular vehicle so that they are hashed to a common value. RSU constantly monitor communication going on among the vehicles and calculate hash value for each pseudonym. In "P2DAP" both RSU and DMV are able to determine whether pseudonyms belong to same pool or not. In this way scheme is able to detect Sybil attack. Scheme works well and privacy of node is preserved until RSU is trusted, if it is compromised then privacy of a vehicle cannot be preserved. Authors gave variations of P^2DAP as C- P^2DAP for detection of Sybil attack, E- P^2DAP for detecting events instead of Sybil attack, T-P^2DAP for detecting collision. As the traffic density varies according to day time so τ-P^2DAP is given to decide threshold for E-P^2DAP and T-P^2DAP while κ-P^2DAP is given to distribute different number of pseudonyms for each RSU based on the traffic nearby those RSUs. By combining all those techniques P^2DAP is an efficient protocol to detect Sybil attack. Only drawback is that the overhead on the DMV.

Mekliche et al. [8] proposed a Sybil attack detection scheme named L-P2DSA which is very similar to scheme proposed by Tong Zhou et al. [10]. In [8] authors overcome drawback present in [10]. The drawback was that when excessive numbers of vehicles are there on the roads DMV becomes bottleneck. To reduce load at DMV, RSU perform additional role of distinguishing between suspicious nodes. A location based technique is used in which position of suspicious nodes is compared and degree of distinction is measured. Simulation result shows that load at the DMV is decreased and the false positive rate also gone down in this scheme.

Chan et al. [7] proposed a scheme named "Footprint", in which authors not only able to detect Sybil attack but also preserve location privacy of the node. In this detection scheme trajectory of vehicle is used while still preserving anonymity and location privacy of vehicle. In this scheme when a vehicle comes into range of a RSU it requests an authorized message from RSU and message is issued by RSU for that vehicle. This authorized message is a proof that this particular vehicle is present at that particular time in its range. Authorized messages can be used to use to identify a vehicle as message would be different at different location. Authorized messages are not directly used because doing so may leak location information of the vehicle. The messages signed by RSU are signer-ambiguous so anonymity is preserved of the RSU. When a vehicle travels through road it collects all the authorized messages to form a trajectory using a public key. In this scheme a vehicle is free to start a new trajectory using a new public key. This freedom can be abuse by the malicious vehicle by generating multiple trajectories to launch Sybil attack. Some observation shows that multiple trajectories generated by malicious vehicle are very alike. In footprint authors established a relationship between these trajectories to detect Sybil attack. Detailed description is given in this work for generating trajectory, location privacy preserving, and establishing relationship with a pair of trajectories.

Hao et al. [4] proposed a scheme to detect Sybil attack which is based on vehicles' geographic information for position based application. This scheme is able to detect common attackers and it also be able to detect smart attacker who are able to adjust their communication range. It is cooperative detection method so every vehicle is cooperating to detect Sybil nodes. The problem of cooperative detection is that the cooperative node should be trustworthy node otherwise result may be deviated. In this method no extra computation devices are needed in detection process because all the communication information are piggybacked in the safety related messages. So this is an efficient detection method. Protocol design for detection has three phases a) probing: In this phase when vehicle broadcast their geographic information they also sent index of nearest M vehicle in front of it and nearest M vehicle behind of it. Index could be something by which a vehicle can be uniquely

identified. Second phase of this protocol is b) Confirmation: Sybil nodes are detected in this phase. Authors mention two type of vehicles as S-vehicle and O-vehicle, S-vehicle are the vehicle which are same side of the suspected vehicle and O-vehicles are the vehicles which are opposite side of the suspected vehicle. If an anomaly is detected, S-vehicle informs this anomaly to others. During this process suspected vehicle is ignored by others. Suspected vehicle is not selected as a verifier in this cooperative message authentication protocol. Authors employ a threshold value on number of S-vehicle and number of O-vehicle for signature protocol. If enough number of S-vehicles are there so that it reaches at threshold signature, O-vehicles are not used. But if there are not enough number of S-vehicles to reach at threshold so O-vehicles are also used to reach at threshold. On the basis of the relative distance between O-vehicle and S-vehicles which detect the anomaly. If a vehicle collects enough partial signatures so it can reach at threshold signature, suspect vehicle is identified. But if it does not reach at threshold signature investigation procedure will stop and the vehicle is treated as a benign vehicle. Third phase of the protocol is c) Quarantine: in this phase all the detected Sybil nodes are quarantine.

Rahbari et al. [6] propose a scheme which is based on cryptography. In this work authors gave a brief introduction to attack which can be performed on VANET and authors also categorize the type of attackers. The schema proposed by the authors cover four security aspects i.e. authentication, non repudiation, privacy and data integrity. Authors consider a scenario as shown in fig 3 and perform detection in that scenario in which A,B,C are the benign vehicles belongs to domain 2 and M is a malicious vehicle which creates a Sybil node S using A's ID. Detection is performed in four phases a) in phase 1 every vehicle should have to register and get a group authentication key by their respective domains. Without this key a vehicle cannot send any message.

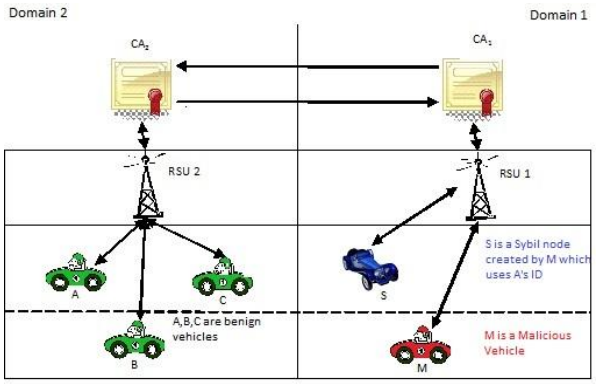

Fig 3: Network Model of [6]

When a vehicle got its authentication key (AK) this key is used to sign the message. This signed message is send to other vehicle and RSU with original message. It is not compulsory for every vehicle to know ids of other vehicles as the message is signed by group authentication key. So the privacy of node is preserved. Receiver verifies sender's identity by signature verification. In the scenario shown in fig 3 there is a malicious node M and a Sybil node S (S is generated by M using A's identity) in the range of RSU1. Following events occur a) S send a message to RSU1. b) at RSU1 as it don't have the private key of CA1 so it cannot decrypt the message. RSU1 send this encrypted message to the CA1 to decrypt OBU id of S. c) in this phase CA1 request private key of A from the CA2 because CA1 cannot decrypt the message signed by vehicle resides in different domain. d) in this phase CA2 reply with the private key of the A to CA1 and CA1 decrypt the message and it is found identical with the original message so S is declared as Sybil node. Problem could be in this scheme is that if malicious node uses the identity of node which is in the same domain then this scheme may fail to detect Sybil attack.

Chen et al. [2] proposed a Sybil attack detection technique which is based on difference between normal and abnormal trajectories of vehicle. This scheme can be used at early development of VANET as it require limited support from VANET infrastructure and in this scheme each node can detect Sybil attack locally. Authors consider that when a vehicle come into range of a RSU it issue a digital certificate with time stamp to the vehicle, so sequence of digital signature form a trajectory. A vehicular node can detect a Sybil node by comparing and analyzing motion trajectory of neighboring node. According to authors the scheme given by them is very robust and have lower system requirement. Detection utilizes the properties of traffic under normal condition for example in normal conditions people drive at their own chosen speed, selects their own path and keep a safe distance from other vehicle. So authors consider that every vehicle have trajectory different from other vehicle. When a Sybil node is created by a vehicle the trajectory of Sybil node and malicious node is found to be identical. So in this work authors make use of trajectories to detect Sybil attack. For example if A and B are the benign vehicle C is malicious vehicle and C' is a Sybil node created by C. When vehicle travels through the road and encountered by different RSU's a trajectory is created by digital certificates issued by RSU's. By comparing trajectories of vehicle Sybil attack can be identified.

3. EXHAUSTIVE INVESTIGATIONS ON SYBIL ATTACK IN VANET

The schemes described above are the summery of work given in recent years in the field of Sybil attack detection. In this section we are giving some comparative analysis of above schemes. As we told earlier that detection scheme may be divided in two categories as centralized and decentralized so here we are indicating which scheme is centralized and which one is decentralized. Privacy of a node is another key issue in VANET so we are considering this parameter also in this table. As we earlier discussed that some schemes uses certificates and some does not, we mention in this table that particular scheme uses certificates or not. RSS another key technique which is used in many detection scheme so we consider it in the table 1.

Table 1: Brief Summary of Schemes Given Above

Authors	Centralize/ Decentralized	Privacy Preserved of a Node or Not	Certification Authority Used or Not	RSS Based	Location Based	Support of RSU	Propagation Model	Detection Rate
Bo Yu et al. [5]	Decentralized	No	No	Yes	Yes	Yes	Shadowing Model	Good
Hussain et al.[9]	Centralized (DMV is the centralized authority)	Yes	Yes	No	No	Yes	-	Good
Bayrem et al. [1]	Centralized (A centralized certification authority which is connected by Road Side Controllers of each domain is the centralized unit)	Yes	Yes	Yes	Yes	Yes	-	-
Tong Zhou et al. [10]	Centralized (DMV is the centralized authority)	Yes	Yes	No	No	Yes	-	-
Kenza Mekliche et al. [8]	Centralized (DMV is the centralized authority)	Yes	Yes	Yes	Yes	Yes	-	Good
Chan et al. [7]	Decentralized	Yes	No	No	Yes	Yes	-	Good (98 % as mentioned in [7])
Hao et al. [4]	Decentralized	Yes	No	Yes	Yes	No	-	-
Rahbart et al. [6]	Decentralized	Yes	Yes	No	No	Yes	-	-
Chen et al. [2]	Decentralized	-	No(Only Digital Certificates are Used at RSU	No	Yes (trajectories contain location information)	Yes	-	Good

4. CONCLUSION AND FUTURE WORK

Most peer-to-peer systems are vulnerable to security attacks. Sybil attack is one of those attacks. In this paper we presented a brief survey of Sybil attack on VANET (a peer-to-peer system). This work could be very useful for the scholars, planning to do some research work on security in VANET. In future we are planning to give a detail survey on some critical attacks which can be performed on VANET.

5. REFERENCES

[1] Bayrem Triki, Slim Rekhis, Mhamed Chammem, Noureddine Boudriga, "A privacy preseriving solution for the protection against Sybil attacks in vehicular ad-hoc networks", Wireless and Mobile Networking Conference, 2013.

[2] Chen Chen, Xin Wang, Weili Han, Binyu Zang, "A robust detection of the Sybil attack in urban VANETs", ICDCS Workshop 2009.

[3] W. Chang, J. Wu, "A survey of Sybil attack in Networks", .Sensor Networks for Sustainable Development, CRC Press.

[4] S. Park, B. Aslam, D. Turgut, Cliff C. Zou, "Defence Against Sybil Attack in Vehicular Ad-hoc Network Based on Roadside Unit Support", In MILCOM, pages 1-7, 2009.

[5] Bo Yu, Chang-Zhong Xu, Bin Xiao, "Detecting Sybil Attacks in VANETs", In: Journal of Parallel and Distributed Computing 73.6 (2013), pp. 746 –756.

[6] Mina Rahbari, Mohammad Ali Jabreil Jamali, "Efficient Detection of Sybil Attack Based on Cryptography in VANET", International Journal of Network Security & Its Applications (IJNSA) (November 2011).

[7] Shan Chang, Yong Qi, Hongzi Zhu,Jizhong Zhao, Xuemin(Sherman) Shen, "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks", Parallel and Distributed Systems, IEEE Transactions on, vol. 23. no. 6, 2012, pp. 1103-1114; DOI 10.1109/tpds.2011.263.

[8] Kenza Mekliche, Dr. Samira Moussaoui, "L-P2DSA: Location-based Privacy-Preserving Detection of Sybil Attacks", 11th international symposium on programming and systems (April 2013), pp. 187-192.

[9] Rasheed Hussain, Heekuck oh, "On Secure and Privacy Aware Sybil Attack Detection in Vehicular Communication", In Journal of Wireless Personal Communication, DOI: 10.1007/s11277-014-1659-5.

[10] Tong Zhou, Romit R. Choudhury, P. Ning, K. Chakrabarty, "P2DAP- Sybil Attacks Detection in Vehicular Ad-hoc Networks", IEEE Journal on Selected Areas in Communications 29(3), 582–594 (2011).

[11] John R. Douceur, "The Sybil Attack", Proc. IPTPS, p.251-260, March 07-08, 2002.

[12] P. Golle, D. Greene, J. Staddon, "Detecting and correcting malicious data in VANETs", Proc. of ACM International Workshop on VANET 2004, pp. 29–37, 2004.

[13] G. Korkmaz, E. Ekici, Urban multi-hop broadcast protocol for inter-vehicle communication systems, in: Proc. of the 1st ACM International Workshop on Vehicular ad Hoc Networks, VANET 2004, pp. 76–85, 2004.

[14] R.M. Yadumurthy, A. Chimalakonda, M. Sadashivaiah, R. Makanaboyina, "Reliable mac broadcast protocol in directional and omni-directional transmissions for vehicular ad hoc networks", Proc. of the 2nd ACM International Workshop on VANET 2005, pp. 10–19, 2005.

[15] J. Zhao, G. Cao, "VADD: Vehicle-Assisted Data Delivery in vehicular ad hoc networks", IEEE Transactions on Vehicular Technology 57 (3) (2008).

[16] KIM, K. H.,CHOI, E. Y., LEE3, S. M., , AND LEE, D. H. "Secure epcglobal class-1 gen-2 rfid system against security and privacy problems", In On The Move (OTM) Workshops, LNCS 4277 (2006), 362–371.