Volume 7, Issue 4, April 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Privacy Aware VANET Security:- Sybil Attack Detection in VANET

Amit Mane
Dept of Electronics & Telecommunication Engineering, M.E Student Full Time VIT Mumbai, Maharashtra, India

Abstract: Vehicular ad-hoc network (VANET) is sub class of mobile ad-hoc network (MANET). MANETS are ad-hoc networks and those types of networks which can alter their location and configure it. Security is the main issue in the network during transmission. Vehicular communication intends to improve the traffic safety for decreasing number of accidents and manages traffic for saving money and time. In vehicular communication, communication between vehicles takes place wirelessly and thus security is an important issue for this kind of network.Vehicular ad hoc network needs such a security architecture which has public safety on the roads.Such Secure architecture should protect it from different types of security attacks and preserve privacy for drivers. One of these attacks against ad-hoc networks is Sybil attack that attacker is creating multiple fake identities that are identities belonging to other vehicles or dummy identities made by the attacker. Attacker is using them for destructive purpose in the network leading to accidents or causing delay in some services for the driver using only one physical device. In this paper we present a various methods for Sybil attack detection in vehicular networks.

Keywords: VANET, Sybil Attack, MANET.

I. INTRODUCTION

1.1 VANET

Vehicular network is a specific type of mobile ad hoc network (MANET).In vehicular ad hoc network vehicles are equipped with onboard unit (OBU) communication devices. VANETs have some different characteristics than MANET like rapid change in topology, no power constraint, large scale, variable networkdensity and high predictable mobility [1]. VANET architecture is designed for vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications.and it consists of two communication devices called the Roadside Unit (RSU) that is placed on the roadside and OBU installed in vehicles. It also recquire some sensors installed on the vehicles for gathering environmental and road information.Dedicated Short Range Communication (DSRC) i.e 5.9 GHZ identified as IEEE 802.11p medium used for communication among vehicles. As it is wireless communications, VANETs are vulnerable to many of the security attacks. One of the most possible attack is Sybil attack introduced by Douceur [2]. In this attack, multiple fake identities created by attacker either by forging new identities or stealing identities from neighboring vehicles.As vehicles within the communication range of sender can overhear its exchanged messages and due to this overhearing identities in message broadcasting stealing can be possible.There are various malicious operations can be done by Sybil attackers in different environments that two major damages by attacker are: Routing:attacker can disrupts routing protocols in VANET.Multi-path routing and geographic routing these two routing mechanism are vulnerable to the sybil attack. Moreover, Sybil attack can also change the head selection mechanism of various cluster-based routing protocols [3]. A VANET turns turn participating car into a wireless router or node which allowing cars 100 to 300 meters of each other to connect and create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile network is created. It is estimated that the first systems that will be this technology are police and fire vehicles to communicate with each other for the purpose of security.The connectivity is done among one vehicle to other vehicle and vehicle to road side infrastructure and vehicle or road side infrastructures to the central authority responsible for the network maintenance.

1.2 Various type of attackers

Insider vs. Outsider

Insider attacker is a member node who can communicate with other members of the network and able to attack in various ways. Whereas, an outsider, who does not have permission to directly communicate with other members of the network, have a limited capacity to perform an attack

Malicious vs. Rational

A malicious attacker damage the member nodes and the network by using various methods without looking for its personal benefit. On the other hand, a rational attacker expects its own benefit from the attacks. Thus, rational attacks are more predictable.

Active vs. Passive

The difference between Active attacker and Passive attacker active attacker can generate new packets to damage the network whereas a passive attacker only eavesdrop the wireless channel but cannot gene rate new packets (i.e., less harmful).

Local vs. Extended

An attacker is considered as local if it has limited access even if it possesses several entities (e.g., vehicles or base stations). Otherwise, an extended attacker increases the limit to access by controlling several entities that are scattered across the network. This distinction is especially important in wormhole attacks that we will describe later.

1.3 Attacks

There are various kinds of attack that can affect the entire system or can degrade the performance of system. The attacks can be categorized into following types.

- **Denial of Service attack**

This strike happens when the aggressor increments control of a vehicle's benefits or jams the channel of correspondence utilized by the Vehicular Network, so it makes tangle to send separating information to its end of the line. It additionally expands the threat to the driver, on the off chance that it needs to rely on upon the application's data. For example, in the event that a malignant needs to make a colossal load up on the roadway, it can make a disaster and use the Dos strike to keep the forewarn from landing at to the approaching vehicles. Creators in [1] talked about an answer for Dos issue and saying that the current arrangements, for example, bouncing don't totally tackle the issue, the utilization of different radio handsets, working in disjoint recurrence groups, can be a conceivable approach yet even this course of action will oblige adding new and more apparatuses to the vehicles, and this will oblige more sponsors and more space in the vehicle. The inventors in, proposed an answer by trading between assorted channels or even correspondence progresses (e.g., DSRC, UTRA-TDD, or even Bluetooth for short ranges), in case they are open, when one of them (routinely DSRC) is chopped down.

- **Message Suppression Attack**

An assailant specifically dropping packets from the system, these bundles may hold discriminating data for the beneficiary, the aggressor stifle these parcels and can utilize them again as a part of other time.

The objective of such an assailant would be to keep enrollment and protection powers from looking into crashes including his vehicle and/or to abstain from conveying crash reports to roadside access focuses. Case in point, an aggressor may smother a blockage cautioning, and use it in an alternate time, so vehicles won't get the cautioning and compelled to hold up in the activity.

- **Fabrication Attack**

An aggressor can make this assault by sending wrong information into the system, the information could be wrong or the transmitter could assert that it is another person. This assault incorporates create messages, warnings, declarations, personalities.

- **Alteration Attack**

An attacker alters an existing data in a network. It includes replaying earlier transmission, alteration of actual entry of the data transmitted, or delaying the transmission of the information .For instance, message is alter by an attacker that “Current road is clear” and send this to other nodes, but actually there is congestion on that place.

- **Sybil Attack**

In this attack node sends multiple messages to other nodes and each message contains a non identical source in such a way that the originator is not known. The main aim of the attacker is to create confusion to other nodes by sending wrong messages and to emphasize other nodes to leave the road for the attacker's benefit.

1.4 Sybil attack

Sybil attack is a one of the critical security issue in vehicular ad-hoc network. It was first introduced by Douceur There are various methods to detect Sybil attack. In Sybil attack one attacker vehicle have control over other Sybil nodes and also have control over other networking protocols. For example The result of some voting based protocols may be deviated because of the presence of sybil nodes and this may also launch Denial of Service attack to disturb the normal operations of data dissemination protocols. Sybil attack can be detected by using three types of techniques

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 attacker node create some fake identities at different position so on the basis of the physical position of the node.

There are various scheme which 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 which issues some form of certificate unique for each vehicles but the schemes which are not centralized in nature use other form of techniques to detect Sybil attack like resource testing or position verification etc.

Meklichenet el proposed a scheme having a 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. We also can use support of RSU which consider as semitrusted unit.

II. SOLUTIONS TO DETECT SYBIL ATTACK

1. Resource testing based method

Resource testing methods test vehicle's resources, such as radio resources,computational and memory resources and identification resources. In radio resource testing methods, each node sends a message for all of the neighboring nodes and then it selects a channel randomly for listening to the response message. If the selected neighbor is authorized, it sends the response in the same channel; otherwise it cannot send the response message for its various Sybil nodes simultaneously on different channels and so Sybil attack is detected.It is not possible for a device to send and receive on more than one channel at a time this assumption we use for radio resource testing method. But in VANETs, attackers may have linked with multiple channels and so this method is not applicable for vehicular network.

In case of identification resource, if the vehicles with MAC and IP addresses that are not recorded in a list, identify as fakes.This method is also not sufficient for VANETs because an attacker vehicle may have multiple fake identities that are not belonging to any of vehicles in the network and it is possible to each of them be registered in the list. Moreover operation of transmitting the registered identities for authorized vehicles violates privacy of drivers. For computational resource testing, vehicles which fails to solve a puzzle are identified as bogus node.Attacker vehicle and its Sybil entities have shared resources such as memory, computational resources, IP and so on. We therefore can detect them with message tracking, monitoring vehicles and finding which vehicles are using shared resources for sending messages and processing of the received signal. This method requires special tools for network monitoring and messagetracking. The goal of using resource testing based methods is not to prevent this attack. Rather, the goal is wrecking this attack and restricting fake identities. But in many cases, attacker can obtain sufficient IDs for its purpose and so a successful attack occurs. Therefore these methods are not suitable for using in VANETs.

2. Posiion verification based method

The methods has one advantage is that a vehicle can be available at only one position at a time. Some of position based approaches are considered for Sybil attack detection, because these methods are available for position based applications like traffic condition reports, collision avoidance,emergency alert, cooperative driving, or resource availability and then it is not compulsory to use extra devices or other method like computational method only for detecting this attack. Security of position information is necessary for working these applications in actual world, because attacker such as pranksters and malicious attackers can impairment the VANET by committing the attacks such as dropping packets, changing existing packets, inserting forged packets and replying packets [6]. [8] localization schemas are divided into 2 categories: range-based and range free methods. In Range-based methods, after guessing distance between a transmitter and receiver, we can use it to find the vehicle's position by using next process. Distance guessing fall into three categories: Received Signal Strength Indicator (RSSI) based methods, time-based methods like Time Of Arrival and Time Difference Of Arrival and Angle Of Arrival based methods [10]. A range free localization method may be used to administer side information as correlate for other position estimations.

3. Encryption and authentication based method

Sybil attack detection is based on the authentication mechanism and public key cryptography in the encryption and authentication meyhods.Lot of research works is going on for sybil attack detection in MANETs and VANETs based on this mechanism [5,20,21]. Using reliable certificates is the only way that has the potential to completely defeat the Sybil attacks. But many of encryption and authentication methods are based on the Public Key Infrastructure (PKI), a heavy and difficult solution that should be tested and evaluated in reality for VANETs. Symmetric key based systems consume less time and memory as compare to Public key encryption or message authentication systems and also require less message size. Therefore, bandwidth and resources consumption increase in case public key systems.

III. SYBIL ATTACK DETECTION BASED ON RSSI

In this section, we propose a received signal strength (RSS) based technique for detecting Sybil nodes in VANET. RSS represents the transmission power minus signal attenuation, which is related to both distance between the transmitter and receiver and environment conditions. Signal attenuation differs significantly from its theoretical expectation, due to many environment factors. Most existing detection approaches give inaccurate result due to the noisy channel and presence of obstacles between transmitter and receiver. These are based on statistical analysis and that is only for static networks. Since our network scenario is not static, existing position verification approaches can not be directly applied for identification of malicious nodes. Proposed approach does not consider the inaccuracies of wireless channel instead it considers the similarity of RSS values of nodes.

In our approach, detection is not dependent on similar RSS values of nodes observed by one RSU, rather all the RSUs cooperatively participate in detection process. These RSUs exchange their observations periodically and if some similar RSS value nodes are observed by RSUs at incremental interval of time, the nodes are regarded as Sybil nodes. Our technique is lightweight because position of nodes are not verified by analyzing received signal strength. Nodes having similar RSS values over significant period of time are considered to be having the same physical trajectory which is possible only for Sybil nodes, as every entity is having unique identity and physical position.

There are some exceptions: Similar RSS values are recorded by RSU if two vehicles coming from opposite direction with similar speeds for some period of time. These two nodes are falsely considered as Sybil nodes. When two vehicles A and B having same distance from R broadcast beacon packets, R stores similar RSS values for both. The observation of single RSU is not able to differentiate the Sybil attack and false positive because of high mobility of

vehicles. Shorter observation period provides inaccurate detection of Sybil attack. It is important to select the proper duration of observation period and number of observers to minimize false positives.

IV. SIMULATION

For visualization of the proposed method JAVA language is used and NetBeans IDE 8.0.2 platform is used. The software requirements of the proposed methods are as follows.

NetBeans Platform:

The NetBeans Platform is a reusable framework for simplifying the development of Java Swing desktop applications. The NetBeans IDE bundle for Java SE contains what is needed to start developing NetBeans plugins and NetBeans Platform based applications; no additional SDK is required.Applications can install modules dynamically. Any application can include the Update Center module to allow users of the application to download digitally-signed upgrades and new features directly into the running application. Reinstalling an upgrade or a new release does not force users to download the entire application again. NetBeans IDE is a free, open-source, cross-platform IDE with built-in-support for Java Programming Language.

NetBeans IDE:

NetBeans IDE is an open-source integrated development environment. NetBeans IDE supports development of all Java application types (Java SE (including JavaFX), Java ME, web, EJB and mobile applications) out of the box. Among other features are an Ant-based project system, Maven support, refactoring, version control (supporting CVS, Subversion, Mercurial and Clear case).

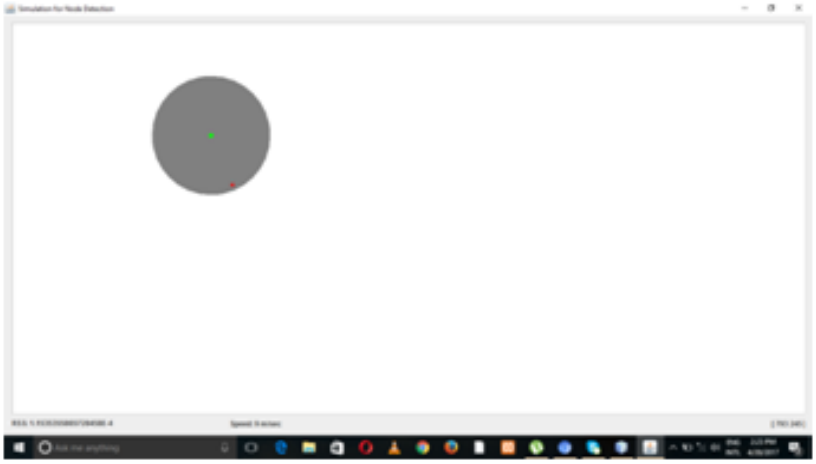

Fig 1.RSS concept

We can detect Sybil attack with the help of RSS concept. In above diagram green dot is a vehicle and red dot is malicious vehicle. The circle indicates the communication range of vehicle. When a vehicle comes at the corner of radius of communication range, it starts communicating. Whenever communication gets start the Received Signal Stregth Indicator also get started. So at start it shows small reading. As vehicle moves forward the RSS value goes on increasing.

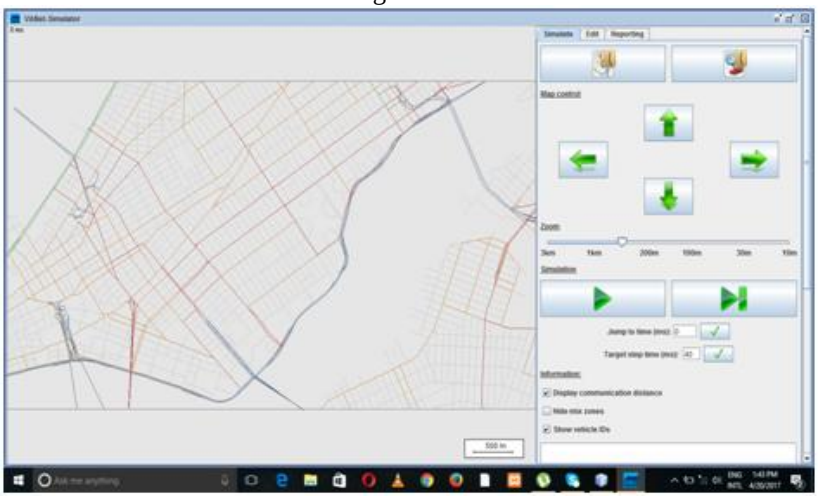

Fig 2. Loading of Map in VANET Simulator

Now malicious vehicle can change the ID.so as soon as that vehicle changes ID and suppose that vehicle is at short distance of Normal vehicle, then whenever malicious vehicle start communication with normal vehicle with new ID then normal vehicle can detect that communicating vehicle is Attacker based on RSS value. Because when malicious

vehicle changes ID and start communication with normal vehicle and as it is at short distance of normal vehicle so it gives large RSS value.So Normal vehicle receives large RSS value with New ID but new ID supposed to be start with Low RSS value.

Now to confirm that whether communicating vehicle is attacker or not, normal vehicle communicates with other vehicles who are in that communication range.It asks to them whether that malicious vehicle was in their communication range or not.If answer is "Yes" then that vehicle is not attacker and if answer is "No" then communicating vehicle is Attacker.

V. RESULT

This paper has implemented the proposed system using Netbean tool. Three metrics are related to network in our evaluation. Network performance metrics are Communication overhead and Sybil attack detection time

Performance Metrics

The follwing performance metrics are considered for assessing the proposed scheme.

Communication overhead: Basically, this metric measures the number of packets exchanged between vehicles and RSUs and between RSUs and the DMV. As will be explained later, we also compare the packet size of our scheme with PKC based scheme that uses RSA cryptosystem

Sybil attack detection time:This metric indicates the time needed to detect a Sybil attack.

1. Communication overhead

We compare our scheme with RSA based eventreporting scheme where vehicles use certified pseudonyms to report events. We measured the number of packets sent from vehicles to the RSU and from the RSU to the DMV at different number of benign vehicles and Sybil attackers. The results are given in Figures 5 and 6 respectively. It can be seen that our scheme has low communication overhead compared with RSA based scheme. This can be attributed to the fact that the symmetric-key encryption generates ciphertext that is shorter the RSA signatures. In addition, the results indicate that the number of packets sent from the RSU to the DMV is significantly less than the number of packets sent from the vehicles to the RSU. This is because the RSUs send the packets to the DMV only when events are reported from same group vehicles. By this way, the DMV is not involved in the decryption of every single event.

2. Sybil attack detection time

The time it takes to suspect a Sybil attack depends on the arrival rate of events, the latency of packet delivery, and the decryption time of the received events. We measured the encryption and decryption time on a host running Linux OS and has a single Intel core CPU of 2.00 GHz and memory of 1.00 Gigabyte. The AES encryption and decryption time of one event is 5 ms and 10 ms, respectively. The packet delivery latency is the time an event packet takes to be sent from the vehicles to the RSU. We found that the average packet delivery latency is 0.17 seconds. Table V gives the taken time to suspect a Sybil attacker at different attacks rate, i.e., an attacker sends an event multiple times using his pool of pseudonyms.

Table 1. Accurary of isolation Sybil attacker with various number of nodes

	20 Nodes	40 Nodes	60 Nodes	80 Nodes
1	86.8143	88.6546	89.8755	93.1465
2	75	77.6216	77.7985	78.231
3	81.4815	85.1651	87.4889	89.455
4	79.165	82.51661	86.1652	88.4964
5	78.6165	81.165156	82.1652	82.7499
6	78.8836	79.651651	79.9899	80.1321

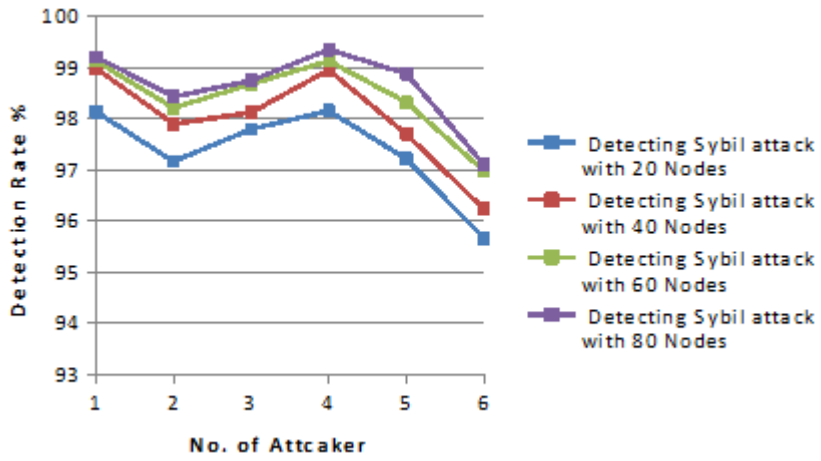

Fig 3. Accurary of isolation Sybil attacker with various number of nodes.

Table 2. Detecting Sybil attack with various number of nodes

	20 Nodes	40 Nodes	60 Nodes	80 Nodes
1	98.1361	98.987987	99.132	99.2121
2	97.1651	97.89797	98.2131	98.431
3	97.7947	98.1214	98.6787	98.7456
4	98.1546	98.955	99.1321	99.3542
5	97.2131	97.69898	98.3213	98.8798
6	95.6547	96.231231	96.9765	97.102

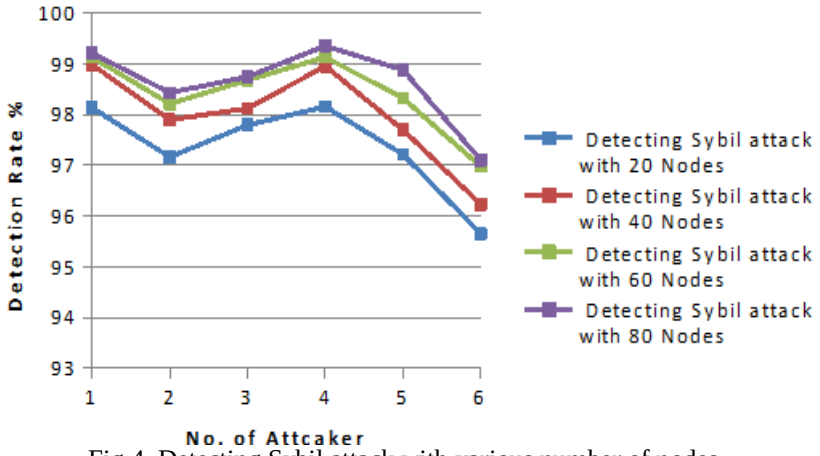

Fig 4. Detecting Sybil attack with various number of nodes

VI. CONCLUSION

The establishment of secure communications within wireless networks remain a key issue because of the vulnerabilities of such environment (mobility, dynamicity, wirelesslinks, lack of infrastructure. Indeed, wireless networks are subject to malicious attacks, such as Sybil node attack : a malicious node creates Sybil entities in the network, able to inject fault and malicious messages. Such attack is very compromising especially within VANET,where the number of nodes and the communication over head are significant. We presented in this report a Sybil detection approach based essentially on received signal strength variations. Our approach allows a node to verify the authenticity of nodes with which it is communicating, via two complementary techniques: the verification of their geographical localizations and the evaluation of their distinguishability degree. We demonstrate through geometrical analysis that verifier nodes can determine precisely which entities are Sybil within VANET, and which malicious nodes create them.To validate our contributions, we carried out analysis, simulations and real tests. We showed that for our localization technique, the choice of the parameters is important to minimize the computed localization error. We showed also that our distinguishability degree metric is significant and efficient to detect Sybil nodes within VANET. Finally, the results of the real tests that we carried out are very promising and validate the real applicability of our contributions.

REFERENCES

[1] Lu, R., Security and Privacy Preservation in Vehicular Social Networks, Doctoral dissertation, University of Waterloo, 2012.

[2] J.R Douceur, "The Sybil attack," Proceedings of the International Workshop on Peer to Peer Systems, 251–260, 2002.

[3] Sood, M., & Vasudeva, A., Perspectives of Sybil Attack in Routing Protocols of Mobile Ad Hoc Network. In Computer Networks & Communications (NetCom), Vol. 131, 3-13, 2013.

[4] Karlof, C., Wagner, D., Secure routing in wireless sensor networks: Attacks and countermeasures, Ad hoc Networks Journal (Elsevier,) vol. 1, 293 -315, 2003.

[5] J. Newsome, E. Shi, D. Song, A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," In Proceedings of the 3rd international symposium on Information processing in sensor networks, 259-268, 2004.

[6] G. Yan, S. Olariu, , M. C. Weigle, "Providing VANET security through active position detection,". Computer Communications, vol. 31, No. 12, 2883-2897, 2008.

[7] B. N. Levine, C. Shields, N. B. Margolin, "A survey of solutions to the Sybil attack," MA, University of Massachusetts: Amherst, 2006.

[8] A. Boukerche, H. A. Oliveira, , E. F. Nakamura, A. A. Loureiro, "Vehicular ad hoc networks: A new challenge for localization-based systems," Computer communications, Vol. 31, No. 12, 2838-2849, 2008.

[9] H. Wang, J. Wan, R. Liu, "A novel ranging method based on RSSI," Energy Procedia, Vol. 12, No. 1, 230-235, 2011.

[10] C.-H. Ou, "A roadside unit based localization scheme for vehicular ad hoc networks," Int. J of Communication Systems Wiley, No. 51, 123-130, 2012.

[11] J. T. Isaac, , S. Zeadally, J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks" Communications IET, Vol. 4, No. 7, 894-903, 2010.

[12] K. Ibrahim, "Data aggregation and dissemination in vehicular ad-hoc networks," Doctoral dissertation, Old Dominion University, Norfolk, Virginia, 2011.

[13] P. Y. Shen, "An efficient public key management regime for vehicular ad hoc networks (VANETS)," Masters by Research thesis, Queensland University of Technology, 2011.

[14] G. Yan, W. Yang, J. Li, V. G. Ashok, "Active position security through dynamically tunable radar," In Mobile Ad hoc and Sensor Systems (MASS), IEEE 7th International Conference, 733-738, 2010.

[15] B. Xiao, B. Yu, C. Gao, "Detection and localization of Sybil nodes in VANETs," Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks, 1-8, 2006.

[16] B. Yu, , C. Z. Xu, B. Xiao, "Detecting Sybil attacks in VANETs," Journal of Parallel and Distributed Computing, Vol. 73, No. 6, 746–756, 2013.

[17] Demirbas, Y. Song, "An RSSI-based scheme for Sybil attack detection in wireless sensor networks," In Proc. Of International Symposium on a World of Wireless, Mobile and Multimedia Networks, 564–570, 2006.

[18] S. Zhong, , L.E. Li, Y.G. Liu, Y.R. Yang, "Privacy-reserving location based services for mobile users in wireless networks," Technical Report. YALEU/DCS/TR-1297, Department of Computer Science, Yale University, 2004.

[19] S. Abbas, , M. Merabti, , D. Llewellyn-Jones, K. Kifayat, "Lightweight Sybil Attack Detection in MANETs," IEEE, Systems Journal, Vol. 7, No. 2, 236-248, 2013.

[20] B. Dutertre, , S. Cheung, J. Levy, "Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust. Technical Report," SRI-SDL-04

