Computer Science and Information Technology 2(4): 197-202, 2014 http://www.hrpub.org
DOI: 10.13189/csit.2014.020403

Sybil Attack Detection in Vehicular Networks

Ali Akbar Pouyan, Mahdiyeh Alimohammadi*

College of Computer Engineering, Shahrood University, Shahrood, 3619995161, Semnan, Iran
*Corresponding Author: m.alimohammadi@shahroodut.ac.ir

Abstract Vehicular communication intends to improve the traffic safety for decreasing number of accidents and manages traffic for saving money and time. In vehicular communication, vehicles communicate wirelessly and so security of this network against attackers should be considered. To become a real technology that has public safety on the roads, vehicular ad hoc network (VANET) needs appropriate security architecture. 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 identities that are identities belonging to other vehicles or dummy identities made by the attacker. Attacker is using them to gain a disproportionately large influence 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 case study of different selective methods for Sybil attack detection in vehicular networks and discuss about advantages and disadvantages of them for real implementation.

Keywords Sybil Attack Detection, Vehicular Ad Hoc Network, Security, Privacy

1. Introduction

Vehicular network is a specific type of mobile ad hoc network (MANET) where the mobile nodes are replaced with vehicles equipped with onboard unit (OBU) communication devices. VANETs have some different characteristics in comparison with MANETs including rapid change in topology, no power constraint, large scale, variable network density and high predictable mobility (vehicles are driving with limited speed in a road with a certain geometric topology) [1]. VANET architecture is designed for vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications with two communication devices called the Roadside Unit (RSU) that is placed on the roadside and OBU installed in vehicles. It also needs to some sensors installed on the vehicles for gathering environmental and road information. The medium used for communications among vehicles is 5.9 GHz Dedicated Short Range Communication (DSRC) identified as IEEE 802.11p. Due to wireless communications, VANETs are vulnerable to many of the security attacks. One of the harmful attacks is Sybil attack introduced by Douceur [2]. In this attack, one attacker creates multiple identities either by forging new identities or stealing identities from neighboring vehicles. Stealing identities can happen by overhearing identities in message broadcasting, as vehicles within the communication range of sender can overhear its exchanged messages. There are numerous malicious operations by Sybil attackers in different environments that two major damages by attacker are:

Routing: attacker can disrupts routing protocols in VANET. Two routing mechanisms vulnerable to the Sybil attack are multi-path routing and geographic routing. Moreover, Sybil attack can also disrupt the head selection mechanism of various cluster-based routing protocols [3]. In multi-path routing, a set of paths that seem disjoint may pass through the Sybil nodes owned by a malicious node. In geographical routing protocols, malicious nodes may appear at more than one place at a time [4].

Voting and Reputation Systems: voting is effective for gathering and verifying some useful information for many of applications that Sybil nodes can change voting result. Reporting and identifying node misbehavior and verifying vehicle position are examples of voting applications.

Due to great damage when this attack occurs, we should have an efficient method for detecting Sybil attack. Defense mechanism for practical implementation should have proper detection rate, minimal time complexity, preserve privacy of drivers and as much as possible not increase exchanging messages in the network. So in this paper we examine different mechanisms for Sybil attack detection and then express some of the selected research works with their features, advantages and disadvantages.

2. Analysis of Defense Mechanisms

We can classify different defense mechanisms in VANETs as: (1) resource testing methods, (2) methods based on position verification, and (3) encryption and authentication based methods. At the following we express some selected works in each domain to consider the problems for implementing each mechanism.

2.1. Defense Based on Resource Testing

Resource testing methods test vehicle's resources, such as radio resources [5], computational and memory resources and identification resources. In radio resource testing methods, each node broadcasts a message for all of the neighboring nodes and then randomly selects a channel for listening to the response message. If the selected neighbor is legitimate, it sends the response in the same channel; otherwise it cannot send the response message for its different Sybil entities simultaneously on different channels and so Sybil attack is detected. Radio resource testing is based on the assumption of it is not possible for a device to send and receive on more than one channel at a time. But in VANETs, attackers may have multiple channels and so this method is not applicable for vehicular network.

For identification resource, if there are vehicles with MAC and IP addresses that are not recorded in a list, identify as fakes [6]. This method is not sufficient for VANETs because a malicious vehicle may have multiple 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 broadcasting the registered identities for legitimate vehicles violates privacy of drivers. For computational resource testing, vehicles failing to solve a puzzle are identified as fakes [6]. Malicious 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 message tracking. The goal of using resource testing based methods is not to prevent this attack. Rather, the aim is undermining 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 sufficient for using in VANETs [7].

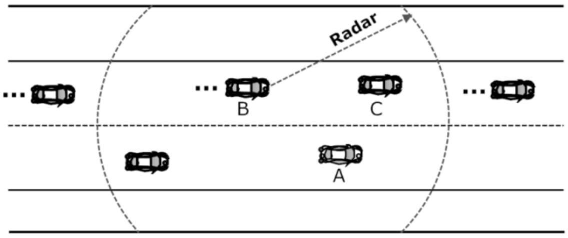

Figure 1. A possible Sybil Attack. *A* obtains *C*'s position as Lc. *A* claims to victim *B* that its position is Lc, and its ID is IDa. *B* detects a vehicle is at Lc then concludes that it is the position of *A* [6].

2.2. Defense Based on Position Verification

The methods are employing this technique, take advantage of this fact: a vehicle can present at only one position at a time. Some of position based techniques are considered for Sybil attack detection, because these methods are available for position based applications including traffic condition reports, collision avoidance, emergency alert, cooperative driving, or resource availability and then it is not necessary to use extra devices or computational methods only for detecting this attack. Protection of position information is necessary for working these applications in real world, because adversaries such as pranksters and malicious attackers can harm the VANET by perpetrating the attacks such as dropping packets, modifying existing packets, inserting bogus packets and replying packets [6].

As stated in [8,9], localization schemas are divided into 2 categories: range-based and range free methods. In Range-based methods, after estimating distance between a transmitter and receiver, we can use it to compute the vehicle's position by using next process. Distance estimation fall into three categories: Received Signal Strength Indicator (RSSI) based methods, time-based methods (e.g. Time Of Arrival (TOA) and Time Difference Of Arrival (TDOA)) and Angle Of Arrival (AOA) based methods [10]. A range free localization method may be used to provide side information as complement for other position estimations. Range-based methods have high accuracy in localization. Therefore we expose range-based methods for the goal of distance estimation and so position verification.

To prevent many of attacks against vehicle position and also Sybil attack, Yan et al. [11] propose a novel method based on the adage: 'Seeing of believing'. In this view the authors use onboard radar as virtual vehicle eye, although the eyesight is limited for the reason of low radar transmission range. So a vehicle can see neighboring vehicles at a limited distance and also it can hear their GPS coordinates reports. With comparison of what is seen with what is heard by the vehicle, it is possible for the vehicle to confirm actual position of neighbors and separates malicious vehicles from the others. There are some problems for using this method: (1) the proposed method requires a new additional hardware that such a device doesn't exist at present [12], (2) the method fails when a target vehicle claims it's at the position of another existing vehicle that both are at the radio range of verifier vehicle [12]. An example of this problem is shown in Fig. 1.

Sybil attack in this situation is not prevented by using this method and (3) as Shen. P [13] has stated, if a vehicle is out of radar range, applying this method is impractical. But in answer to this problem, Yan et al. in [14] state that radar range in Yan et al. [11] method, is assumed to be constant, so if a target vehicle is out of verifier vehicle radar range, this approach uses intermediate vehicles. But using intermediate vehicles is potential for security problems [14]. For gaining trusted and safe position information about target vehicle, it is necessary to use more than one vehicle as intermediates. But if many of intermediate vehicles are malicious players, verifier vehicle will be fooled (this problem is possible with collusion attack).

The problem of constant radar range is solved in Yan et al. [14]. The purpose of this research work is enhancing position security and reducing response time. Authors proposed an onboard radar system that is dynamically configurable. In this method, if target vehicle (target for receiving position information) is out of verifier vehicle radar range, radar can dynamically tune its range by changing the signal sample size and so verifier vehicle at the most time can get the position information directly rather than using intermediate vehicles. Therefore vehicle positioning system is improved and last problem in Yan et al. [11] method has largely been solved, but other problems still remain.

Xiao et al. [15,16] proposed a lightweight method for detecting and localizing Sybil nodes in VANETs. Operation of this method is locally and distributed around the vehicle. The verifier confirms claimed position of each vehicle. In this approach, statistical analysis of received signal strengths taken by neighboring vehicles over a period of time are used to calculate position of the claimer vehicle. This simple method with low overhead and low accuracy has a 10 meters error range in positioning and if neighbor vehicles are Sybil entities, this method is vulnerable against spurious signal strength measurements. Therefore Xiao et al. have proposed an improvement. In this improvement, each vehicle has the role of claimer, witness or verifier on different occasions and for different purposes. The claimer vehicle periodically broadcasts its position and identity information and verifier vehicle confirms the claimer position by using a set of witness vehicles. For witness selection, reliable vehicles should be selected. So for witness selection, the authors use traffic pattern and RSU support in two following rules: (1) each vehicle receives a position certification when passes through an RSU. This certificate that is contains a time stamp, the passing vehicle's identity and position of the RSU, proves presence of the vehicle near the RSU at a certain time, and (2) all of the selected witnesses should be in the opposite road direction of the claimer. By combining these two rules, witnesses are the physical and legitimate vehicles on opposite sides of the road, excluding any Sybil vehicle. They used rule 2 because if the claimer is a Sybil entity generated by a malicious vehicle, the other Sybil entities from the same malicious vehicle cannot use the malicious certificates to prove their physical presence.

Advantages of this method are: (1) it is suitable for applying on sparse RSUs and so has a low cost architecture, (2) no additional hardware is required in this approach, and (3) detection rate is larger than 99%. Disadvantages of this approach are: (1) non-sufficient accuracy for position detection with received signal strength measurements in dense roads, (2) it is possible to there are not sufficient number of vehicles on opposite side of the road and also using this method in one-way roads is not possible, (3) privacy violation with broadcasting identity and position information for distributed position verification.

RSSI is a low cost method for hardware-constrained systems, in which the distance between two entities is estimated based on the received signal strength and using theoretical radio propagation models. The reliability of the estimated RSSI cannot be guaranteed in environments with multipath and shadowing effects for the reason of attenuation in the received signal. There are some techniques that register RSSI values with vehicle identifier for detection of Sybil entities [17-19]. These methods may be sufficient for detecting some attackers in the network, but we cannot use them as a single defense mechanism. Because in many of researches some of assumptions for using this approach are restrictive: malicious vehicles do not collude with each other and sender vehicles do not increase or decrease their transmission rate. These two assumptions may happen in VANET and so if we assume that attacker is very smart, this method is not sufficient for implementation as a single mechanism.

2.3. Defense Based on Encryption and Authentication

In the encryption and authentication methods, Sybil attack detection is based on the authentication mechanism and public key cryptography. Many of research works are proposed for attack detection in MANETs and VANETs based on this mechanism [5,20,21]. Using trusted certificates is the only approach that has the potential to completely eliminate 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. Public key encryption or message authentication systems consume more time and memory than symmetric key based systems and also increase the message size. Therefore, bandwidth and resources consumption increase in public key systems.

Chang et al. [22] proposed a new protocol based on the authorized messages as vehicle trajectory, which is called Footprint. This protocol preserves the privacy of the vehicles in the network. In this protocol when a vehicle encounters with each RSU, upon request, receives an authorized message from the RSU and thus presence of the vehicle will be proved at a specific time. For unique vehicle identification, each vehicle collects a set of consecutive authorized messages from the RSUs is passing by them. These authorized messages chain together and form a trajectory for the vehicle. To reduce computational complexity, only the last RSU signs the vehicle trajectory (chained authorize messages). RSUs can track each vehicle with a set of its authorized messages; therefore in this protocol there are two conditions that help vehicles to remain ambiguous in the network. In first condition all of the RSUs that sign the vehicle's messages, are unknown or authorized messages are signer-ambiguous and so with eavesdropping of the authorized messages it is not possible to detect a specific vehicle. In another condition, authorized messages are temporary linkable. This means two messages issued by one RSU are recognizable if and only if they are issued within the same period of time. This condition is necessary because sometimes without even knowing which RSU has signed the authorized message, malicious vehicle can detect trajectory of the vehicle by gathering authorized messages by the same

RSU over the time. With this condition vehicle trajectories cannot be used for a long time. These two conditions guaranteed that this scheme has position-hidden feature and preserves vehicle privacy. Sybil attack detection in this scheme is an online process that independently is done by a vehicle or RSU in the role of conversation holder which initializes a conversation amongst vehicles. All of the vehicles participating in a conversation send their trajectories to the conversation holder for verification. Conversation holder makes a graph from all of the trajectories and with investigating similarity between each pair of trajectories, if trajectories are very similar attack can be detected. If some trajectories are similar together, attack possibility is high because malicious vehicle and Sybil entities constitute a complete sub-graph in the main graph, Sybil attack certainly will be detected. This method is evaluated in an urban scenario with the detection rate of 98%. Advantages of this method are: (1) In this protocol vehicles are unknown for each other, (2) The only requirements for vehicles are a commercial GPS receiver and DSRC wireless communication module [7], But limitations of this protocol are: (1) identification of a complete graph in a graph consists of the trajectories has exponential complexity, (2) if malicious vehicles have high mobility and high speed, they can create longer trajectories and probability for detecting of Sybil trajectories decreases. Because number of subsets in a long trajectory with more RSUs is more and so finding similar trajectories is more difficult, (3) this method is vulnerable if some of RSUs are compromised, because they issue any number of authorized messages for malicious vehicles so as to be distinct.

There is another protocol that uses trajectories for Sybil attack detection [23]. This protocol doesn't need to public key infrastructure. Because in early stage VANETs only a small percentage of the vehicles on the road are smart and equipped to devices for V2V and V2I communications and also only the most essential infrastructure components are present not a VPKI for certifying the vehicles. In this research similar to Footprint [22], vehicles receive temporary certificates driving through RSUs. Sybil attack detection is with the fact of spatial and temporal correlation between vehicles and RSUs. In this research two methods are proposed based on the type of certificates issued by RSUs.

First method is series of timestamp certificates in Fig. 2. In this method each vehicle receives a set of temporary timestamp certificates showing trajectory and time when it is passing through RSUs. Each timestamp certificate is an aggregated certificate constituted of prior and current certificates issued by neighbor RSUs for this vehicle. The main process is checking similarity between aggregated timestamp series of different vehicles. Two similar timestamp series show a Sybil attack.

Second method is temporary certificate in Fig. 3. In this method each RSU issues temporary key pairs and certificates for each vehicle for only a limited time and particular local area covering by the RSU. For issuing the first certificate for each vehicle, some RSUs should be equipped to camera or other devices for physical authentication. After receiving the first certificate and temporary key, upon certificate update request by vehicles to the next RSUs, they binds new key pair and certificate to previous certificates (hash values of previous certificates) and make chained certificate. Each vehicle uses this certain temporary certificate for a single spatial interval and so Sybil attack with uniqueness of certificate is preserved. This model has a physical part for issuing the first certificate and so should be implemented with more analysis and discussion.

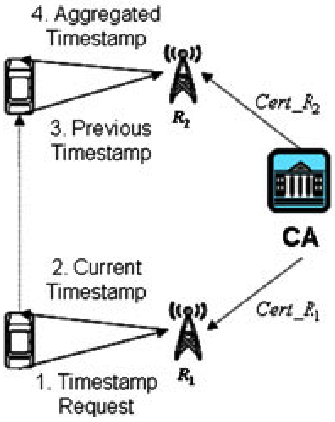

Figure 2. timestamp series based approach [23].

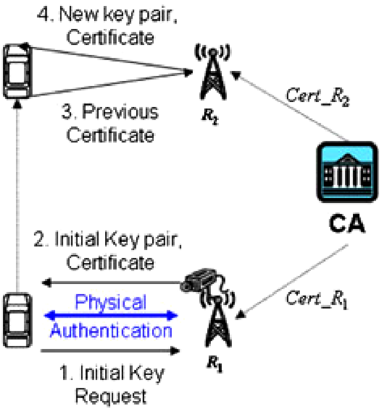

Figure 3. temporary certificate based approach [23].

We can compare these two methods. Advantage of timestamp series based approach is no needing to physical authentication for the first visit with RSUs. But temporary certificate approach needs to some of RSUs be equipped to extra devices for initial authentication. If we use all of RSUs equipped to physical authentication, this is costly and if we use some RSUs, first certificate not be issued until the vehicle meets an equipped RSU and so network is vulnerable in this time interval. Disadvantages of timestamp series approach are: (1) it requires to a precise deployment of RSUs in urban areas for the reason of complex roadways. Because if we consider Fig. 4, a vehicle *V* is passing through R1 and R2 and it can attempt to obtain at least two different certificate series from roadside unit R3, because both R1 and R2 are adjacent to R3. Therefore two paths are created by a vehicle and vehicle *V* success to create a Sybil entity. In this paper for preventing of misusing with creation of a secondary path by a malicious vehicle, it's necessary to install an RSU for each path ending to an intersection that increases costs in urban areas, (2) traffic messages are gradually extended and this increases time of message authentication. But in second approach (Temporary certificate model) traffic messages have a shorter length, and (3) similar to Footprint, this method is evaluated in an urban scenario. But using of this approach in the roads or highways with direct paths that have few intersections should be investigated because probability of similarity among separate trajectories in these roads is high and so false-positive goes up.

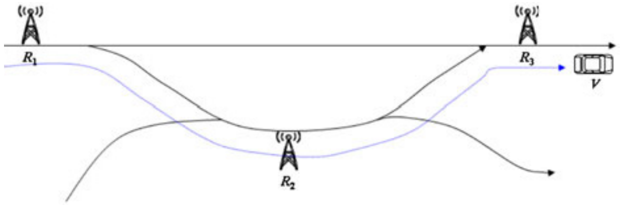

Figure 4. Example of a complex roadway [23].

In [24], authors propose a scheme with the name of P2DAP (Privacy-preserving Detection of Abuses of Pseudonyms). In this approach, Department of Motor Vehicle (DMV) generates a sufficient number of yearly pseudonyms for all vehicles. Generated pseudonyms are grouped in two steps. In step 1, DMV hashes each pseudonym with a global key and then selects a set of bits from hash result. Selected bits are called "coarse grained hash value". All of the pseudonyms with the same coarse grained hash value is called coarse grained group. In step 2 DMV separately hashes each pseudonym with another key that is known by just DMV and selects a set of bits from hash result that called "fine grained" hash value. Equal fined grained hash values are inserted in a subgroup of the same coarse grained hash value. It means all of pseudonyms with one value of fine grained hash are into a subgroup belonging to a specific coarse grained group.

DMV distributes the global key used for generating coarse grained hash values, to all of the Road-side Boxes (RSB) and preserve the key used for generating fine grained hash values securely and private. RSBs in this research work are the same RSUs in previous methods. After generating sufficient number of fine grained hash values in each subgroup of coarse grained group, all of the pseudonyms in each subgroup (with equal fine grained and coarse grained hash values) should be allocated to one vehicle. DMV assigns a unique fine grained subgroup of pseudonyms to each vehicle at the time of yearly vehicle registration and so this unique mapping is a secure plate number for each vehicle. Sybil attack detection is done in two levels. At the first, RSBs overhear exchanging messages and puts the used pseudonyms for signing a specific event, into a list and with calculation of coarse grained hash values of these pseudonyms, all of the pseudonyms with repetitive coarse grained hash values mark as suspicious and RSB send them to the DMV. DMV generates fine grained hash values from these pseudonyms and if they have the same value of fine grained hash, attack is inevitable.

In this research pseudonyms are used for the privacy preserving goal and RSB cannot specifies a certain vehicle in a coarse grained group because if RSB is compromised, the attacker only obtains the coarse grained hash key from compromised RSB (fine grained hash key is just known for DMV). In this method RSBs perform the most of DMV tasks for reducing communication overhead. For more security, authors suggest to use a multi-level hash instead of one-level hash. In initial version, all of Sybil vehicles can be detected. Other versions of this schema are proposed with decreasing of communication and computation overhead in exchange for reduction in attack detection rate. It's a good research because in many of works privacy is preserved as long as the RSB can be trusted. Compromising of RSBs is considered in this work and RSBs are semi-trusted parties. But there are some of the problems in this approach: (1) initial infrastructure for registering of vehicles and Sybil attack detection make it difficult to use this approach, especially for vehicles are traveling between different countries with different VANET standards (2) this method may fail in colluding attacks [25], (3) DMV services aren't designed for heavy network traffic. Excessive communication cause to DMV becomes a bottleneck [25].

3. Comparison

It is not possible to firmly select a unique mechanism and method. Selection of a good method for detecting Sybil attack depends on the allocated costs, road architecture and number of vehicles in each country. Features of the existing methods can help to choice a suitable method. So In real world a good method meets the following requirements: (1) detection a large percentage of Sybil nodes for eliminating damage in VANET, (2) necessary time for discovering and removing of Sybil entities is an important factor that should be minimal, (3) privacy of drivers should be preserved, (4) doesn't need to additional high priced hardware, and (5) doesn't increase exchanging messages in the network.

We have not proposed resource testing methods, since they are not sufficient methods for Sybil attack detection with high accuracy in VANETs. Many of position verification methods are simple, have less computational complexity than authentication methods and they are distributed in processing. These are positive features for implementation. But they violate privacy and expose position and identifier information of vehicles. Moreover, distributed processing by vehicles in these methods, lead to messaging overhead. All of the authentication methods need an infrastructure for key distribution, revocation and so on. This infrastructure also may be necessary for many of other applications such as secure message exchanging, group communications, etc. In these methods privacy preserving and higher accuracy are positive features although they are complex for implementation and usually have less scalability than position verification methods.

4. Conclusion

In this paper, we have discussed about defense methods against Sybil attack in VANETs. According to the studies in this area, each method has some advantages and disadvantages for implementing. Resource testing methods are not sufficient to implement for Sybil attack detection with high accuracy in VANETs. Authentication methods are more reliable and useful for message integrity, authenticity and privacy and there are suitable methods in this category for practical implementation in urban areas. In contrast, position verification methods are lightweight and easy for implementation and if they have high accuracy for position verification, we can use them for other security purposes such as position verification after receiving location information that periodically broadcast by vehicles for position related applications. So selection between two recent methods is depending on policies, requirements and allocated cost in each country.

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] M. 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-04-02, SRI Int’l 2004.

[21] S. Capkun, , L. Buttyán, J. P. Hubaux, “Self-Organized Public Key Management for Mobile Ad Hoc Networks,” IEEE Trans. Mobile Computing, Vol. 2, No. 1, 52-64, 2003.

[22] S. Chang, , Y. Qi, H. Zhu, J. Zhao, X. Shen, “Footprint: detecting Sybil attacks in urban vehicular networks,” IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 6, 1103-1114, 2012.

[23] S. Park, B. Aslam, D. Turgut, C. C. Zou, “Defense against Sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support,” Security and Communication Networks, Vol. 6, No. 4, 523–538, 2013.

[24] T. Zhou, , R. R. Choudhury, P. Ning, K. Chakrabarty, “P2DAP—Sybil Attacks Detection in Vehicular Ad Hoc Networks,” Selected Areas in Communications, IEEE Journal, Vol. 29, No. 3, 582-594, 2011.

[25] M. A. Razzaque, A. Salehi, S. M. Cheraghi, “Security and Privacy in Vehicular Ad-Hoc Networks: Survey and the Road Ahead,” Springer Berlin Heidelberg, In Wireless Networks and Securit, 107-132, 2013.