ISSN 2277-3061

Comparative Study on Sybil Attack Detection Schemes

S. Hamdan[1], R. S. Al-Qassas[2], and S. Tedmori[3]
Department of Computer Science. Princess Sumaya University for Technology
Amman, Jordan
[1]salamhamdan1990@gmail.com
[2] raad@psut.edu.jo
[3] s.tedmori@psut.edu.jo

ABSTRACT

Vehicular Ad Hoc Network (VANET) is a wireless network formed between a collection of vehicles connected through wireless connections. VANETs can help increase the passengers' comfort, safety, efficiency and convenience by providing them with information about the ongoing road status and other relevant road information. VANETs, similar to other networks, face numerous security threats. One such threat is the Sybil attack, a critical threat that can impair the proper functioning of VANETs. In a Sybil attack, a malicious node illegitimately claims multiple identities and simultaneously exploits these fake identities in order to disturb the functionality of the VANET by disseminating false information. In the presence of a Sybil node, any kind of attack can be launched on the VANET. This paper provides a comprehensive review and comparison of the different techniques that have been proposed in the literature to prevent or reduce the adverse effects of Sybil attacks.

Keywords

VANET; Sybil Attacks; Network Security; Wireless Networks.

1. INTRODUCTION

VANET is a subclass of Mobile Ad-Hoc Network (MANET) in which nodes are vehicles. VANET differs from MANET in its architecture, challenges, characteristics and applications. With the use of a Dedicated Short Range Communication (DSRC), VANETs are capable of providing wireless communication between moving vehicles and Road Side Units (RSUs) [1]. In VANET there are two forms of communications: Vehicle to Vehicle (V2V) and Vehicle to RSU (V2R) [2]. VANET is a self-organized network; it does not need any centralized control and is built up by moving vehicles. Any node in the network can act like a router, and play an important role in the discovery and maintenance of the route from source to destination [3].

VANETs have many applications. VANET applications fall under three broad types, namely: safety oriented applications, convenience oriented applications, and commercial oriented applications. Safety oriented applications [4, 5] help drivers in avoiding potential danger. Such types of applications also take care of both the roads and drivers safety. Examples of such applications include intersection violation warning, on-coming traffic warning, and traffic signal violation warning. Convenience oriented applications [5, 6] can help in maintaining road efficiency, saving the driver's time and money. Examples of such applications include intersection management, parking availability, and congested road notification. Commercial oriented applications [5, 6] provide the drivers with entertainment and services, such as media or map download.

The nature of VANET makes it vulnerable to various serious types of attacks [7] such as the Sybil node attack, in which a vehicle fakes the identities of multiple vehicles. As an illustration, consider the case of a greedy driver who fakes a number of false identities, creating the impression of a traffic jam, causing other drivers to choose alternate routes. Moreover, Sybil nodes may also initiate Denial of Service (DoS) attacks, in order to hinder the successful data transfer between two moving vehicles [8]. This paper provides a comprehensive overview of Sybil attack detection schemes in addition to a comparison between these schemes based on their merits. To the best of our knowledge, no such comparison has been made.

The rest of the paper is organized as follows. Section II describes the security requirements in VANETs. Section III includes a description of the attackers in VANETs. Section IV describes the attacks on VANETs. Section V includes a description of the Sybil attack detection schemes and a comparison between them. Finally, section VI concludes the paper.

2. SECURITY REQUIREMENTS IN VANET

In order for VANET applications to work properly, the following general security requirements should be present:

- Entity identification: Entity identification requires that each entity participating in the VANET network must have a unique identify, but entity identification does not mean that each entity must prove its actual identity [9].
- Entity authentication: Entity authentication imposes that each entity must verify that it is whom it claims to be [10].
- Privacy preservation: Privacy in VANET is attained when the two related goals of untraceability and unlinkability are achieved. Untraceability implies that the adversary cannot identify that a given set of actions were performed by the same entity. Unlinkability implies that it is not possible for the intruder to link vehicle´s identity to that of its owner [9].
- Confidentiality: Confidentiality to guarantee that the message only be read by the sender and the receiver [11].
- Integrity: Integrity to ensure that the content of all messages is protected in order to prevent their content from being altered or modified by an intruder [11].
- Availability: Availability implies that at any time the entity is able to send or receive messages [12].
- Data trust: Data trust to ensure the data integrity and accuracy of the information [9].

3. ATTACKERS IN VANETS

Before providing an overview of the attacks that can occur in VANET, a discussion of the attacker's types is provided. Depending on the behaviour of attacker, the attack types can be classified into four categories as described below [7, 13, 14]:

- Insider vs. Outsider: An insider attacker is an authenticated member that possesses a certified public key, and can communicate with other members in the network. An outsider attacker, on the other hand, is perceived as an intruder to the network, so he has a limited ability and hence can launch limited types of attacks in comparison to the insider attacker.
- Malicious vs. Rational: A malicious attacker aims to harm the functionality of the network and other nodes in the network, without seeking personal benefits. A rational attacker, on the other hand, seeks personal benefits, making the attack method and the attack target more predictable.
- Active vs. Passive: An active attacker generates signals or packets and causes serious damage to the data or information by altering it; whereas, apassive attacker monitors the transmission signal for the message contents.

- Local vs. Extended: A local attacker is considered local if its scope is limited, even if he possesses several entities. An extended attacker widens its scope by controlling several entities that are scattered across the network.

4. ATTACKS IN VANETS

VANETs are vulnerable to various types of attacks, which can be classified according to the security requirements. These include attacks on non-repudiation, attacks on privacy, attacks on availabilty, miscellaneous threats such as brute force attack and social attack, and finally attacks on identification and authentication [7, 9, 14, 15]. Fig. 1 summarizes these attacks and provides examples on them.

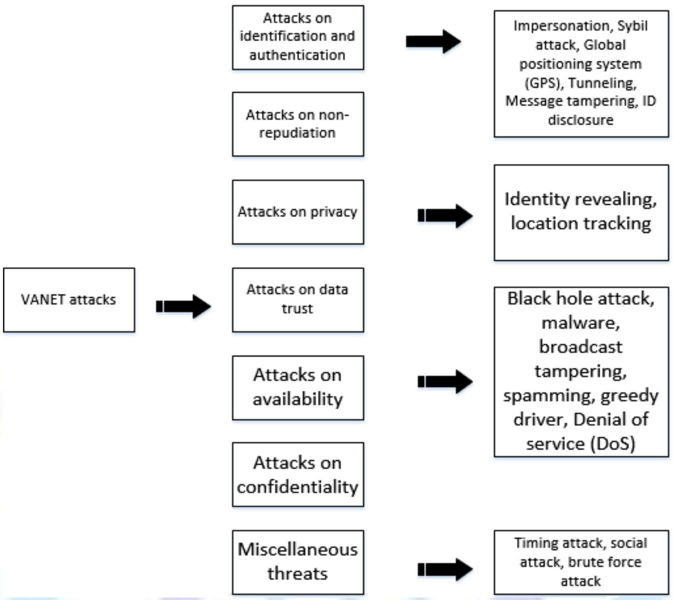

VANET attacks
Attacks on identification and authentication
Attacks on non-repudiation
Attacks on privacy
Attacks on data trust
Attacks on availability
Attacks on confidentiality
Miscellaneous threats
Impersonation, Sybil attack, Global positioning system (GPS), Tunneling, Message tampering, ID disclosure
Identity revealing, location tracking
Black hole attack, malware, broadcast tampering, spamming, greedy driver, Denial of service (DoS)
Timing attack, social attack, brute force attack

Fig. 1: VANET attacks

The focus of this paper is on Sybil attacks which belong to the attacks on identification and authentication. For the sake of clarity for the reader, below is a list all the attacks that belong to this category.

1) *Impersonation* is an attack where the intruder node may gain admission to the network management system, and claim to be a legitimate node, making changes on the system configuration. This enables the attacker to gain unauthorized access by guessing the identity and authentication details of an authorized node. A typical example is the man-in-the-middle attack, in which the attacker can read and modify messages communicated between two nodes. For example, when two nodes, let's say A and B, are directly communicating with each other, the attacker can pretend to be node B with respect to node A, and vise versa, without letting either of them know that they have been attacked [16].

2) *False attribute possession* is a subtype of impersonation. In this type of attack, the attacker, pretends that he possesses an attribute in order to get some benefits.An example of this is when a normal vehicle claims to be a police patrol [17].

3) *Replay attack* is when an attacker resends previously sent information. This occurs when the attacker captures a generated frame and uses it in other parts of the network [7, 15].

4) *Global Positioning System (GPS) Spoofing* occurs when each vehicle knows its location via the GPS. In this attack, the attacker uses a GPS simulator that generates signals stronger than the signals generated by a genuine satellite. The signals generated are faulty, so the driver receives wrong location information [15].

5) *Tunneling* is when the attacker connects two separated Ad hoc networks with each other, using an extra communication channel as a tunnel. The attacker can then perform traffic analysis or selective forwarding attack [7].

6) *Message tampering* occurs when a message that contains valuable and critical information is tampered by the attacker by either modifying, dropping, or corrupting it [15].

7) *ID disclosure* is a passive attack, where the attacker sends malicious code to a specific node, which collects the vehicle's ID and current location. The collected data can be used for instance by car rental companies to track their own cars [13].

8) *Sybil attack* is a type of impersonation attack, where the attacker uses different identities at the same time [18].

5. SYBILATTACK DETECTION SCHEMES

Sybil attack detection schemes are categorized into three categories, namely: radio resource testing, position verification and cryptography based.

5.1. Radio resource testing

Radio resource testing mechanisms are designed on the assumption that each node has a limited number of resources. A legitimate node must have a certain number of resources. Therefore, the Sybil node can be detected by computing the number of resources. If the number of resources is less than the usual number then the node is considered a Sybil node, otherwise it is a trusted node [19]. However, since a Sybil node can easily have more resources than a legitimate node, this approach is not suitable for VANETs [20].

5.2. Position verification

Position verification techniques rely on the verification of the node's position and that each position is associated with only one identity. The following solutions are classified as position verification solutions.

Yan et al. [21] proposed a solution named Position Active Security through Seeing (PASS). The solution assumes that the radar is acting as the "eye" of the scheme. Although the radar has a low transmission range, the vehicle can see beyond its range through exhanging information with the neighboring vehicles. Therefore, it can see what the neighboring vehicles see. The proposed solution is based on a comparison between what a node can see and what its neighbors can see through exchanged information in order to detect malicious nodes and confirm the actual position of neighboring nodes. This solution makes an assumption that 85% of the nodes are legitimate. Furthermore, the approach suffers from long communication delays and long response times in addition to other potential security issues.

Yan et al. [22] proposed a technique named Tunable radar to handle the communication delay in the PASS technique. Tunable radar uses a dynamically tunable radar instead of static radar. The radar range is changed by increasing the sampling rate. The PASS scheme assumes that the cells are created on the roads before hand with a cell range of 200m, and that vehicles map to their respectives cells using GPS coordinates. Vehicles within a local cell can communicate directly with each other. The simulation results have shown that the tunable radar technique enhances the efficiency of detecting position and also prevents potential position attacks in a local cell compared to PASS. The idea of using local cell methodology, is to keep verifying the position information within the cell, which will decrease the bandwidth usage, delay and computational overhead.

Xiao et al. [23] proposed a solution that depends on the signal strength captured by the neighboring vehicles. In this solution, nodes are classified into three classes: claimer, witness, and verifier. A claimer node claims its position, by sending a beacon message periodically. A beacon message contains information such as: NodeID and Beacon sequence number, position, neighboring list, and signature. The neighboring list contains: NodeIDs, Beacon number, and received signal strength. A witness node receives the claimers' beacon messages, measures the signal strength for each claimer, and then saves them in its memory. When this node becomes a claimer, it will broadcast the measured signal strength for each claimer in its beacon message.A verifier node collects all the received signal strength from witness nodes, and calculates the position of the claimer nodes. If the difference between the claimed position and the calculated position is large then the claimer is considered a suspicious node.

To solve these problems, Xiao el al. [23] proposed a scheme that takes advantage of the road infrastrucure and base station support in the vehicular surroundings. This scheme assumes that each vehicle has a verified identity and that roadside units are sparsely distributed along roads, so each vehicle will receive a position certification when it passes by a base station. This certification contains a timestamp and the position of the base station to verify the presence of the node near the base station at specific time. Hence, when two vehicles come from opposite directions, they can prove to each other that they came from a certain base station. All witness nodes should consist of nodes in the opposite direction of the claimer node. Few limitations are associated with this scheme. It has limited accuracy due to the use of signal strength approach; which makes it uncapable of detecting some attacks as it cannot distinguish between two nodes that are close to each other. Furthermore, a malicious node can fool the detection system by using a model to compute the required transmission signal strength for the needed position.

Yu et al. [8] improved on the work proposed in [23], by increasing the efficiency of position estimation against the fake position of the Sybil node, so it can effectively improve the estimated claimer's position. This algorithm takes the signal strength measurments and corresponding position to estimate the position. However, the results obtained in [8] indicate that the accuracy is still low. This scheme attempts to fix the two problems of improving the accuracy that the witness is a real node not a sybil node, and proving that the node honestly claimed its position. To solve the first problem, the authors assume that the nodes are equiped with a Presence Evidence System (PES), which is designed to prove when and where a node comes from, so that only physical vehicles can remain as witnesses. They also assume that the base stations are sparsly distributed along the road, so that every vehicle that passes by a base station will issue a certificate that contains: the vehicle identity, timestamp and the position of the base station. Also in this scheme, all witness nodes should consist of nodes in the opposite direction of the claimer node. To solve the second problem, a statistical detection method was used to ensure that the node's claimed position is a real one by increasing the observation period to collect more signal strength readings.

Grover et al. [18] proposed a Sybil attack detection technique in which each node in the network, whether it is an RSU or a vehicle exchanges information in order to detect the Sybil nodes. Each node includes its position and timestamp within the message. When a node receives the message, it will verify the claimed position, either by computing the estimated position through received signal strength, or by position verification approach [24]. If the estimated position matches the claimed position, then the node generates an observation that it is a real node not a Sybil node, and forward it to the neighbouring nodes, otherwise it gives no response. Each observation has a timestamp, and it describes the node's trajectory. Each node stores its observations in a table, and these observations are broadcasted in the network. In this table, entries are sorted according to timestamp, if two entries are the same, then one of these nodes is a Sybil node. In this technique, each node in the system will exchange each observation it makes so the delay time in this techneque is high. Another limitation is that a malicious node can fool the detection system by using a model to compute the required transmission signal strength for the needed position.

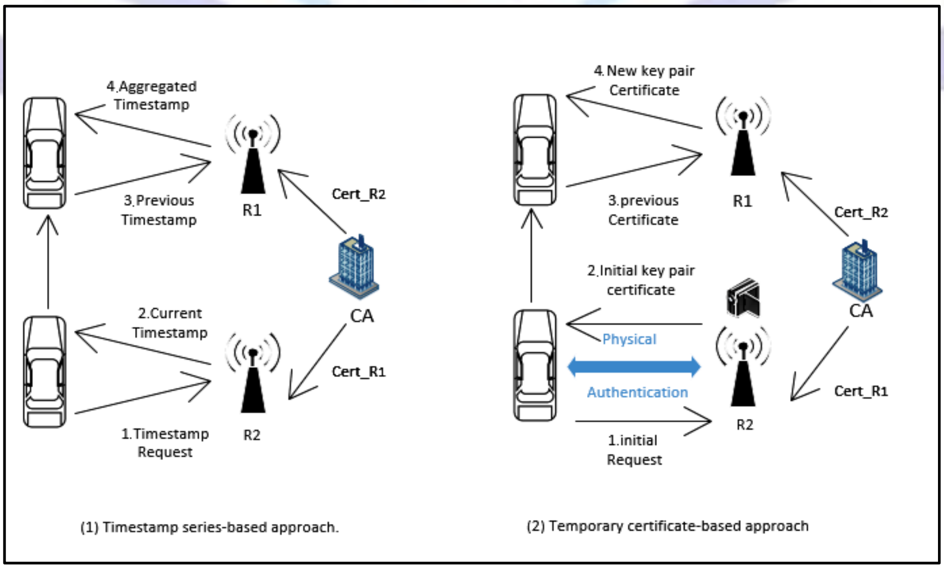
5.3. Defences Based on Encryption and Authentication

These methods include encryption and decryption of the message using symmetric, asymmetric keys, or digital signature. They also guarantee the reliability of the position and identities claimed by the vehicles. The following solutions fall under this category.

Chang et al. [19] proposed the footprint scheme that uses the trajectories (path) of vehicles for identification. The anonymity and location privacy of the vehicle are preserved. The RSU issues an authorization message to each vehicle that passes by it. This authorization message identifies the vehicle and verifies its presence. In order to reduce the message size, only the last RSU signs the vehicle trajectory. Since vehicles can be in different areas, they can get different authorization messages. This method guarantees vehicle location privacy using a location-hidden authorization message scheme. The RSU signature on the messages is ambiguous, preventing the RSU location from being revealed. Footprint has the advantage of ensuring the anonymity of the vehicle as it does not require the use of vehicle ID. However it requires the existance of a trust authority and that roads must be equipped with RSUs.

Park et al. [25] proposed a solution based on two methodolgies that depend on the type of certificate. The two methods are illustrated in Fig. 2. The solution architecture consists of certificate authority (CA) and RSUs. The CA is responsible for issuing certificates of RSU's public key. The public key of the CA is available on vehicles on board units. Unlike the previous scheme, the vehicle needs to register with a trust authority. So the RSU is the only component who issue the certificates. This solution is based on the timestamp series certificate approach and the temporary certificate approach, which are described as follows:

- *Series of timestamp certificate approach:* Each RSU in the network generates certificates that contain the current timestamp marked by the RSU. When the vehicles pass by RSUs they obtain a series of timestamp certificates, showing their trajectories. The Sybil node can be detected if two vehicles have the same timestamps, bcause it is unlikely that two vehicles pass by a sequence of RSUs with the same timestamps. Many challenges face this approach if applied in urban environment. The first challenge is the complexity of the roads. The second challenge is that since urban environment has a many road intersections, vehicles tend to slow down or stop at these intersections, so vehicles are likely to have similar timestamps, which will make Sybil node detection difficult. To solve this problem RSUs should be deployed on the edges.
- *Temporary certificate approach*: Each RSU generates key pairs on a temporary basis to be valid for a short period of time. A vehicle should be authenticated by an RSU in order to get the first certificate, after that, the vehicle renews its key pair and certificate with the next RSU resulting in a chained certificate. With this appraoch, the chances of detecting a Sybil node is higher when compared to the other approach that depends on one certificate at a time.



(1) Timestamp series-based approach.

(2) Temporary certificate-based approach

Fig. 2: Basic ideas of proposed approaches[25]

Zhou et al. [26] proposed a scheme named Privacy-Preserving Detection of Abuses of Pseudonyms (P2DAP). In this scheme, the communication depends on Road Side Boxes (RSBs), which are similar to the RSUs, and are used to reduce the communication overhead. The solution is based on the assumption that there are adequate pseudonyms generated through the Department of Motor Vehicle (DMV) for all vehicles. The pseudonyms are generated and grouped following the two steps shown in Fig. 3. In the first step, DMV hash pseudonyms in one-way global key K_c; DMV distributes K_c to all RSBs in the network. Then DMV selects a group of bits named coarse-grained hash value, to organize the pseudonyms according to these bits. The pseudonyms with the same coarse grained hash value are named coarse grained group. In the next step, each pseudonym is hashed with another key K_f that is only known by DMV, and then the DMV selects a group of bits named fine-grained hash value. Finally, this group is sub-grouped into fine-grained group.

DMV will keep generating pseudonyms, until an adequate number of fine-grained values are generated. Each sub-group is allocated to one vehicle. So each vehicle has a unique fine-grained sub-group, which can be thought of as a secure plate number for the vehicle. In order to detect a Sybil node, the RSBs overhear the exchanged messages and put the used pseudonyms in a list. Then, the RSBs calculate the coarse-grained hash value for each one. If an RSB realizes that two pseudonyms have the same coarse-grained hash value, the node is considered as a potential Sybil node; after which, the RSB sends a report to the DMV. The DMV in turn produces the fine-grained hash values from the pseudonyms; if the values are the same, then a Sybil node is detected. The advantage of this scheme is that the node’s privacy is preserved. However, it is not designed for heavy traffic. Moreover, this method is not adequate for vehicles traveling between countries, because each country has its own VANET standards [20, 27].

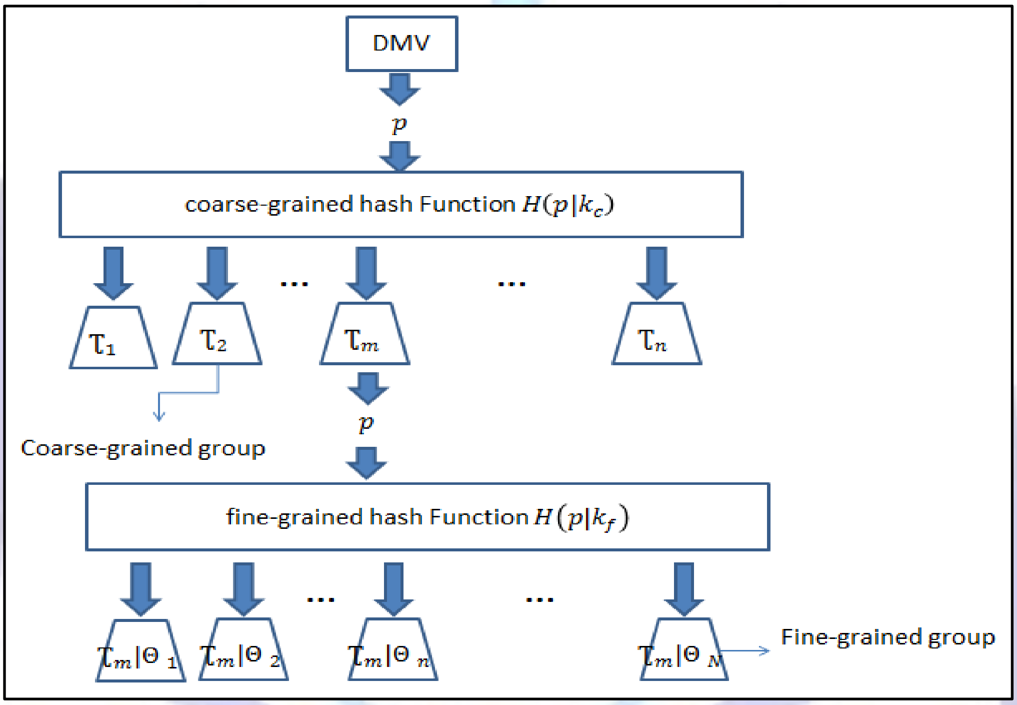


Fig. 3:Generation and two-level hashing of a pseudonym [26]

Rahbariet al. [28] proposed a detection scheme based on a fixed key infrastructure. This method focuses on authenticating the node before it sends any message transmission. The detection scheme is done in two phases. In the first phase, each vehicle is registered in a group, and it will receive a public Authentication Key (AK). When a vehicle wants to send a message, the message will be encrypted and signed with the AK. The signed encrypted message will be sent along with the original message, and the receiver will verify the authority of the node by the signature verification performed by decrypting the message with the AK. In the second phase, since the RSU initially does not have the private key of the node, it sends a request to the local CA. Similarly, since the local CA does not have the private key, it will send a request to retrieve the private key from the home CA (CAh). The communication between CAs is performed through a secure channel, so the local CA will decrypt the signed encrypted message and compare the decrypted result with the original message in order to detect the Sybil node. In this scheme, most of the operations are done in the CA, so the delay is short. However, if the vehicle moves to another region, the Sybil attack detection does not work proberly.

A detailed comparison between Sybil attack detection schemes have been conducted based on the following merits: the cost, the accuracy of detecting the Sybil nodes, the time efficiency in detecting the Sybil node, support of highways environment, support of urban environment, support of privacy and extra bandwidth usage. Radio resource testing based schemes; have been excluded from this comparison as they are inadequate in VANETs. Table 1 describes the merits of these schemes.

Table 1: A comparison between Sybil attack detection schemes

Sybil attack detection scheme	Low cost	Accuracy	Detection time efficiency	Highways environment	Urban environment	Privacy of drivers	Low Bandwidth usage
Yan et. al. [21]	X	X	X	√	X	X	X
Yan et. al. [22]	X	X	√	√	X	√	X
Xiao et. al. [23]	√	X	√	√	X	X	X
Yu et al. [8]	√	√	√	√	√	X	X
Grover et al. [18]	√	X	X	√	√	X	X
Chang et al. [19]	√	X	√	√	X	√	√
Park et. al. [25] Timestamp series approach	X	√	X	√	√	√	√
Park et. al. [25] Temporary certificate approach	X	√	X	X	√	√	√
Zhou et al. [26]	X	√	√	√	√	√	√
Rahbariet al. [28]	X	√	√	√	X	√	X

6. CONCLUSIONS AND FUTURE WORK

This paper identifies the VANETs security requirements and the various possible attacks in VANETs. Sybil attack detection schemes are classified into three categories: radio resource testing, which is inadequate in VANETs, position verification schemes, which try to bind one identity with one position, and encryption and cryptography schemes that use symmetric, asymmetric keys, or digital signatures. A comparative study between exiting popular Sybil detection schemes is provided based on their merits. As part of our future work, the authors plan to conduct an experimental evaluation study for these schemes using simulation.

REFERENCES

[1] Al-Sultan, S., Al-Doori, M.M., Al-Bayatti, A.H., and Zedan, H.: 'A comprehensive survey on vehicular Ad Hoc network', Journal of network and computer applications, 2014, 37, pp. 380-392

[2] Grover, J., Gaur, M.S., Laxmi, V., and Tiwari, R.K.: 'Detection of incorrect position information using speed and time span verification in VANET'. Proc. Fifth International Conference on Security of Information and Networks, 2012, pp. 53-59

[3] Ranjan, P., and Ahirwar, K.K.: 'Comparative study of vanet and manet routing protocols'. Proc. International Conference on Advanced Computing and Communication Technologies (ACCT), 2011, pp. 517-523

[4] Kamini, K., and Kumar, R.: 'Vanet parameters and applications: A review', Global Journal of Computer Science and Technology, 2010, 10(7), pp. 72-77

[5] Mittal, N.M., and Vashist, P.: 'A Detail Survey on Applications of Vehicular Ad hoc Networks (VANETs)', International Journal of Computer Science and Mobile Computing, 2014, 3(6), pp. 713-721

[6] Kumar, V., Mishra, S., and Chand, N.: 'Applications of VANETs: Present & Future', Communications and Network, 2013, 5(1), pp. 12-15

[7] Rawat, A., Sharma, S., and Sushil, R.: 'VANET: security attacks and its possible solutions', Journal of Information and Operations Management, 2012, 3(1), pp. 301-304

[8] Yu, B., Xu, C.-Z., and Xiao, B.: 'Detecting sybil attacks in vanets', Journal of Parallel and Distributed Computing, 2013, 73(6), pp. 746-756

[9] Fuentes, J.M.d., González-Tablas, A.I., and Ribagorda, A.: 'Overview of security issues in Vehicular Ad-hoc Networks': 'Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts' (IGI Global, 2011), pp. 894-911

[10] Wasef, A., Lu, R., Lin, X., and Shen, X.: 'Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]', IEEE Wireless Communications, 2010, 17(5), pp. 22-28

[11] Kargl, F., Ma, Z., and Schoch, E.: 'Security engineering for vanets', Proc. 4th Wksp. Embedded Sec. in Cars, 2006, pp. 15-22

[12] Plößl, K., Nowey, T., and Mletzko, C.: 'Towards a Security Architecture for Vehicular Ad Hoc Networks'. Proc. Seventh International Conference on Availability, Reliability and Security, 2006, pp. 374-381

[13] Raya, M., and Hubaux, J.-P.: 'Securing vehicular ad hoc networks', Journal of Computer Security, 2007, 15(1), pp. 39-68

[14] Sumra, I.A., Ahmad, I., Hasbullah, H., and bin Ab Manan, J.-L.: 'Classes of Attacks in VANET'. Proc. Saudi International Electronics, Communications and Photonics Conference (SIECPC), 2011, pp. 1-5

[15] Dhamgaye, A., and Chavhan, N.: 'Survey on security challenges in VANET', International Journal of Computer Science and Network, 2013, 2(1), pp. 88-96

[16] Rai, A.K., Tewari, R.R., and Upadhyay, S.K.: 'Different types of attacks on integrated MANET-Internet communication', International Journal of Computer Science and Security, 2010, 4(3), pp. 265-274

[17] Porwal, V., and Patel, R.: 'A survey of VANETs: The Platform for Vehicular Networking Applications', International Journal of Advanced Research in Computer Engineering & Technology, 2014, 3(8), pp. 2801-2805

[18] Grover, J., Kumar, D., Sargurunathan, M., Gaur, M.S., and Laxmi, V.: 'Performance evaluation and detection of sybil attacks in vehicular Ad-Hoc networks': 'Recent Trends in Network Security and Applications' (Springer, 2010), pp. 473-482

[19] Chang, S., Qi, Y., Zhu, H., Zhao, J., and Shen, X.: 'Footprint: Detecting sybil attacks in urban vehicular networks', IEEE Transactions on Parallel and Distributed Systems, 2012, 23(6), pp. 1103-1114

[20] Pouyan, A.A., and Alimohammadi, M.: 'Sybil Attack Detection In Vehicular Networks', Computer Science And Information Technology, 2014, 2(4), pp. 197-202

[21] Yan, G., Olariu, S., and Weigle, M.C.: 'Providing VANET security through active position detection', Computer Communications, 2008, 31(12), pp. 2883-2897

[22] Yan, G., Yang, W., Li, J., and Ashok, V.G.: 'Active position security through dynamically tunable radar'. Proc. IEEE 7th International Conference on Mobile Adhoc and Sensor Systems (MASS), 2010, pp. 733-738

[23] Xiao, B., Yu, B., and Gao, C.: 'Detection and localization of sybil nodes in VANETs'. Proc. Dependability Issues in Wireless Ad hoc Networks and Sensor Networks, 2006, pp. 1-8

[24] Leinmuller, T., Schoch, E., and Kargl, F.: 'Position verification approaches for vehicular ad hoc networks', Wireless Communications, IEEE, 2006, 13(5), pp. 16-21

[25] Park, S., Aslam, B., Turgut, D., and Zou, C.C.: 'Defense against sybil attack in vehicular ad hoc network based on roadside unit support'. Proc. IEEE Military Communications Conference (MILCOM), 2009, pp. 1-7

[26] Zhou, T., Choudhury, R.R., Ning, P., and Chakrabarty, K.: 'P2DAP—Sybil attacks detection in vehicular ad hoc networks', IEEE Journal on Selected Areas in Communications, 2011, 29(3), pp. 582-594

[27] Razzaque, M., Salehi, A., and Cheraghi, S.M.: 'Security and privacy in vehicular Ad-Hoc networks: survey and the road ahead': 'Wireless Networks and Security' (Springer, 2013), pp. 107-132

[28] Rahbari, M., and Jamali, M.A.J.: 'Efficient detection of sybil attack based on cryptography in vanet', International Journal of Network Security & Its Applications, 2011, 3(6), pp. 185-195