Journal of Computers Vol. 29 No. 2, 2018, pp. 1-6
doi:10.3966/199115992018042902001

A Survey on Sybil Attack Detection in Vehicular Ad hoc Networks (VANET)

Zaid A. Abdulkader[1,2], Azizol Abdullah[2*], Mohd Taufik Abdullah[2], Zuriati Ahmad Zukarnain[2]

[1] Al Iraqia University, Baghdad, Iraq

[2] Faculty of Computer Sciences and Information Technology Universiti Putra Malaysia, Selangor, Malaysia

azizol@upm.edu.my

Received 17 October 2016; Revised 7 March 2017; Accepted 30 March 2017

Abstract. The Vehicular Ad hoc Networks are a special type of ad hoc network, which along with lacking in infrastructure, contain communicating entities that move with different accelerations. Hence, this obstructs the establishment of more consistent end-to-end communicating pathways and efficiently transferring data. Therefore, the VANETs display many network concerns and show differing security challenges for obtaining a secure communication, ubiquitous connectivity, and reputed management systems that can affect the cooperation and the negotiation between the various mobile networks. This survey report studies some techniques reported by the researchers for the detection of the Sybil attack in the VANET systems.

Keywords: intrusion detection system, mobile ad hoc network, Sybil attack, vehicular ad hoc network

1 Introduction

The Vehicular Ad hoc Networks (VANET) are a special type of the Mobile Ad-hoc Networks (MANET) which can communicate between the neighbouring vehicles and the roadside equipment [1-3]. In the VANET network, the vehicles act as the communicating nodes which belong to the self-organising mobile network with no knowledge regarding anyone else's presence and without any prior screening. These networks contain two node types: On-Board Units (OBUs) and the Road Side Units (RSUs). The OBUs are the radio devices which are installed in the moving vehicles; whereas the RSUs are installed on the roadside and contribute towards the network infrastructure. The RSUs act as the router between all the vehicular traffic. With the help of the Dedicated Short Range Communication (DSRC) radio devices, the OBUs link the vehicles to the RSUs [4]. Recently, it is seen that the VANETs are developing into one of the most appropriate mobile technologies. They are seen to be a very promising approach for the implementation of the wireless mobile technology. Also, it is a promising approach for implementing the Intelligent Transportation System (ITS). The VANETs are seen to differ from the MANETs significantly: they have a higher node mobility, a larger scale of mobile networks, a more dynamic and geographically constrained topology, a very strict deadline, slower deployments, unreliability in the channel conditions, sporadic node connectivity, a recurrent network fragmentation and driver behaviours [1-2, 5]. The main objective of the VANET technology is allowing a good communication between the vehicles. Hence, the nodes have to incorporate the radio interfaces for efficient communication. Also, a particular range spectrum has to be committed for exchanging the data in the VANET technology. For a node to become an important part of the VANET technology and communicate effectively, it needs certain specific features that help it collect information and inform the neighbours along with making appropriate decisions using the gathered information. These features include the cameras, sensors, Global Positioning

* Corresponding Author

System (GPS) receivers, on-board computers, Event Data Recorders (EDRs) and the omnidirectional antennas [6]. The VANET technology has some advantages, like a decrease in the road accidents, better driving and travel experience, simplified payments processes for the tolls, fuel and parking etc. The road users make use of several applications for their safety and efficient driving, traffic management, warnings, music sharing, infotainment, comfort, maintenance, and for network gaming [7]. All these applications require a large exchange of the messages regarding the traffic problems, emergency message distribution, warnings about the road condition which improve the traffic safety and ensure driving efficiency. Hence, an effective data communication is needed between the nodes. The message content could greatly affect the driver behaviour, which could indirectly affect the network topology, thus, impacting the security is any malicious user is seen to alter the messages [8]. Some attacks, like the Sybil attack result in traffic jams, cheat the position data and also spread a lot of false data [2].

2 Overview of the Sybil Attack

The Sybil attack is a kind of spoofing or impersonating attack wherein the attacker is seen to spoof the identity of one node in the mobile network and therefore, all messages that are directed towards the attacked node are now transmitted to the attacker [9]. There exist many types of impersonating attacks like the Invisible Node Attacks, Stolen Identity Attacks, and the Sybil Attacks. In the case of the Sybil attack, the node which is used for the impersonation of the other network nodes is known as the malicious node or the Sybil attacker, while the node whose identity is spoofed is known as the Sybil node. Fig. 1 describes one such Sybil attack. Herein, the Sybil attacker is seen to create an illusion depicting a traffic jam on a road. In the VANET condition which involves the occurrence of an accident on the highway, the vehicle which observed the accident first, sends route change or deceleration warning messages to the other vehicles. The receivers then forward the messages to warn the other followers. The Sybil attack could tamper this kind of forwarding process and the vehicles are not able to forward the messages, thus, affecting and endangering the passengers and the drivers. It is seen that if the number of the Sybil attacks in the network increase, then they can control the complete network. The number of the Sybil nodes that are created by any Sybil attacker is dependent on the storage, communication and the computational resource of the attackers.

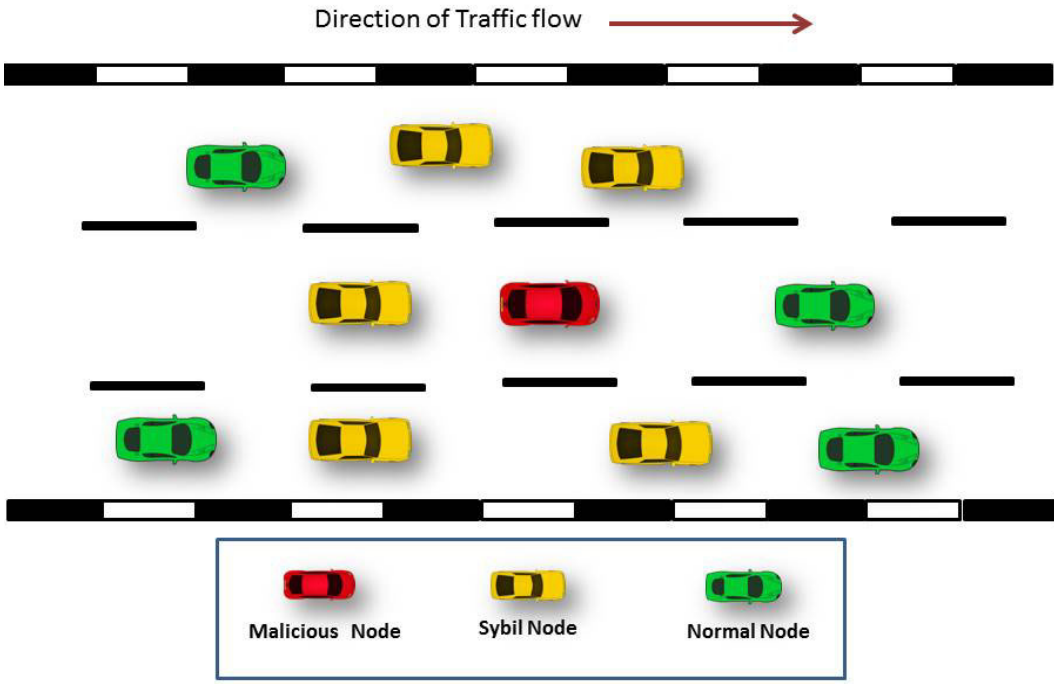

Fig. 1. Sybil Attack

3 Literature Survey

In their study [10], Feng et al. proposed the Event-Based Reputation System (EBRS), wherein the dynamic reputation and the trusted value for every event was employed for suppressing the distribution of the false messages. The EBRS detects the Sybil attacks having stolen identities and fabricated identities for communication. The technique is also seen to defend against the Sybil attacks as every event had a specific reputation value and a trusted value. The authors suggested the EBRS technique for defending against the Sybil attacks and they also considered the multiple sources of the false identities. For privacy protection, the vehicles sent messages using pseudonyms rather than their real identities. After the verification of the vehicle's local certificate, the EBRS technique detects the Sybil attacks having theft or forged identities. Furthermore, to defend against the future Sybil attacks, the EBRS technique established a reputation and a trusted value in the VANETs. It is seen that if the dynamic reputation and the trusted values are below their corresponding threshold values, the message regarding the event is not spread, thereby suppressing the distribution of the false data.

In their paper [11], Bruno et al. suggested the use of an anonymous decentralised privacy-preserving, authentication and *Sybil* attack detecting protocol for the VANETs called as the *ASAP* -V (*Authentication and Sybil Attack detection Protocol for VANETs*). Their results indicated that the *ASAP* -V was quite robust against the *Sybil* attacks, having a lesser than average detecting time as compared to the state-of-the-art works, along with no false-positive or false-negative detection. The authentication procedure in the protocol is dependent on a multiple-pseudonym scheme for providing a position privacy for the users, while the non-repudiation process can be achieved using the Group Signature Scheme. Additionally, the approach used the anonymity set theory in the multilevel fashion for detecting and avoiding the *Sybil* attacks, along with providing a privacy control to the users at the same time.

In their paper [12], Yu et al. investigated the probability of applying the signal strength distribution analysis for the detection of the Sybil attacks. Initially, they designed a cooperative detecting technique, wherein multiple neighbouring nodes were seen to cooperate for measuring the signal strength distribution of the suspicious nodes and thereby verify its physical location. They used the Random Sample Consensus (RANSAC)-based algorithm for increasing the robustness against the outlier data which was fabricated by the Sybil nodes. However, this primary cooperative technique was seen to offer a very limited amount of accuracy. Furthermore, the technique was vulnerable towards the fabricated estimations by the Sybil nodes. For applying this cooperative technique for the VANET technology, it is important to certify that the signal strength estimations are seen to originate from the actual physical nodes rather than the fabricated type of Sybil nodes. For solving this problem, the authors suggested the idea of Presence Evidence System (PES). The PES helped them ensure that all the nodes used in opposite traffic were actual nodes and could serve as trustworthy sources for the signal strength estimations. The system was seen to fully benefit from all the inherent VANET technology features like road topology, high mobility, and indirect support from the roadside infrastructure. Furthermore, the authors also noted that this algorithm was able to gather better signal strength estimations after extending the period of observation, thus improving the accuracy of the detection. This led them to propose a statistical detection technique, which performed hypothesis analysis on the collected measurements and also judged if the measurements matched a normal pattern of distribution pattern. When the distribution pattern becomes inconsistent with regards to its alleged physical position, a Sybil node is reported.

In their study [13], Hussain et al. considered a privacy-friendly *pseudonymless* technique as the reference for their two-fold technique for detecting and/or preventing the Sybil attacks in VANET. In the case of the high-frequency Scheduled Beacons (SB), the authors used the Tamper-Resistant Module (TRM) for carrying out the pre-assembly study on the beacons, whereas they proposed using the RSU-based Sybil attack detecting technique for the Event Reporting Messages (ERM). The vehicles are seen to obtain the tokens from the nearby border RSUs while in motion and utilise them for reporting any event happening in the surrounding area which falls under the jurisdiction of the domains which house the issuing Border RSUs (BRSUs). The vehicular nodes have to report the event only at one time and use one token for every event. It is seen that the carrying out an early lightweight pre-assembly investigation on the beacons decreased the Sybil attacks threats that were launched by the exploiting SBs.

Grover et al., proposed the technique which is seen to exploit the features of the Sybil node, as the neighbours having fake identities (originating from the malicious nodes) shared important common neighbouring nodes [14]. The researchers exploited the primary features of the Sybil attacker i.e., using

the forged identities in a simultaneous manner for differentiating the malicious node from the legitimate node. The suggested approach was seen to follow the primary assumption that any 2 vehicles should not have the same exact nodes as the neighbouring nodes for the longest time duration except when there was a high vehicular density. The fake identities, which were created by the Sybil attacker, were bound to the same physical instrument and shared the same set of neighbouring nodes simultaneously.

In one other study, Saggi et al. attempted to isolate and detect the Sybil attack on the different vehicles, thus resulting in the network proficiency [15]. This scheme worked in 2 different phases. The first phase saw the node registration by the RSU after their credential identification. If the nodes were verified successfully, the second phase began and it allocated identification to the vehicles. In this fashion, the RSU was seen to gather relevant data from the neighbouring nodes and also defined the threshold speed limit and also verified whether the threshold values exceeded the defined speed limits. It was seen that multiple identities which were generated by the Sybil attack were very harmful to the networks and could be used wrongly for distribution of false information over the complete network.

Step 1: Define the network having a specific number of RSUs and vehicles. The particular vehicle number and the identification number gets defined in the registered data. All RSUs can access this registered data. The server stores all the data regarding the vehicles, while the RSUs also contain all data regarding the vehicles.

Step 2: Any new vehicle joining the network has to send a 'Hello' message to the RSU. Thereafter the RSU asks the node for its identification number.

Step 3: The RSU verifies the node identity and stores all its information. It then defines the vehicular speed and compared its threshold value to the pre-defined speed limits of the vehicles.

Step 4: After successfully verifying the identification numbers, the RSU gathers all relevant data regarding the adjacent or neighbouring nodes of all the registered nodes. The RU then defines the speed limits of the vehicles on the roads on which the vehicle is registered.

Step 5: If any malicious node sends a 'Hello' message to the RSU, then, the RSU registers that malicious node, however upon verification, the RSU can detect that the neighbouring node differs from the legitimate node. Thus, the malicious nodes are detected from a network. For verification of this detection process, the RSU floods the network with the monitor mode messages and then, the neighbouring nodes of that malicious node starts scrutinising the malicious node and detect whether it is malicious or not.

Step 6: Stop.

In their study, Grover et al. applied the simulations for studying the manner in which the VANET performance is affected by the Sybil attackers and their node mobility [16]. The Sybil attack is detected by observing the behaviour of the nodes by the adjacent nodes present in the network. Thereafter, these nodes transmit their observations within themselves. Their observations include verifying:

(a) whether the number of the data packets obtained from the specific nodes is higher than the threshold value

(b) whether a majority of these packets are obtained from the same position or trajectory.

Lal et al. suggested an improved CP2DAP scheme, which is a scheme that detected the Sybil attacks with the help and cooperation of the Central authorities and a set of specific RSUs [17]. Their modification in the original scheme involved the region authority-based collaborative process for the detection of the Sybil attacks along with a revocation process which uses the Bloom filters for preventing any more attacks from the malicious nodes. This form of Sybil attack detection does not need the vehicle identity and hence, it is seen to preserve the privacy of the vehicle. After detecting the Sybil attack, the identities of the malicious vehicles are revoked in order to prevent any kind of further attack. The technique uses a revocation method which uses the Bloom filters or the Compressed Certificate Revocation Lists (C2RL). The bloom filters are seen to decrease the communication overhead involved in the transmission of the whole Certificate Revocation Lists (CRL) to the vehicles present in a network.

Mohammadi et al. suggested a secure protocol for resolving the issue involving the privacy of 2 conflicting goals along with Sybil attacks in Vehicle-to-Vehicle (V2V) communication in VANET [18]. This protocol was seen to be based on the Boneh-Shacham (BS) short group signature approach and the batch verification. The authors suggested their technique based on the lightweight group signature approach, which was seen to ensure a privacy preserving condition for the V2V communications. The proposed scheme also used a speedy verification procedure for the batch signatures, which makes use of the Boneh and Shacham (BS) method that requires a short time a provides a secure group communication.

Lastly, the technique which was used for the revocation checking in the BS signature scheme and was used for checking the double registration in the location-based services was proposed by the authors for detecting Sybil attacks in the VANETs.

4 Conclusion

Many studies have noted that the VANETs are one of the most promising and also challenging research topics in the intelligent transportation systems due to their safety and non-safety related services which ensure maximal comfort for the drivers and the passengers. However, due to their frequent topology changes, higher mobility and numerous security attacks, implementing the VANET technology is a challenging task. The VANET technology is seen to be vulnerable to many security attacks depending on the broadcast infrastructure. We have discussed numerous malicious Sybil attack detecting approaches in our paper. Based on the analysis, we can conclude that in order to confront the increasing security challenges, many novel detection schemes have to be proposed.

References

[1] A.-S. K. Pathan (Ed.), Security of Self-organizing Networks: MANET, WSN, WMN, VANET, Auerbach, Boca Raton, 2010.

[2] Y. Wang, F. Li, Vehicular Ad Hoc Networks, in: S. Misra, I. Zhang, S.C. Misra (Eds.), Guide to Wireless Ad Hoc Networks, Springer, London, 2009, pp. 503-525..

[3] W. Chen, J. Yu, X. Liu, The Design of Electronic License Plate Recognition Terminal System Based on nRF24LE1, in: 2012 Fifth International Symposium on Computational Intelligence and Design (ISCID), 2012.

[4] S.N. Pathak, U. Shrawankar, Secured Communication in Real Time Vanet, in: 2009 2nd International Conference on Emerging Trends in Engineering and Technology (ICETET), 2009.

[5] H. Hartenstein, L.P. Laberteaux, A Tutorial Survey on Vehicular Ad Hoc Networks, IEEE Communications Magazine 46(6)(2008) 164-171.

[6] A. Stampoulis, Z. Chai, A Survey of Security in Vehicular Networks, Project CPSC 534 (2007).

[7] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan, Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges, Telecommunication Systems 50(4)(2012) 217-241.

[8] T. Leinmuller, R.K. Schmidt, E. Schoch, A. Held, G. Schafer, Modeling Roadside Attacker Behavior in Vanets, in: GLOBECOM Workshops, 2008 .

[9] J. Grover, D. Kumar, M. Sargurunathan, M.S. Gaur, V. Laxmi, Performance Evaluation and Detection of Sybil Attacks in Vehicular Ad-Hoc Networks, in: International Conference on Network Security and Applications, 2010.

[10] X. Feng, C.-Y. Li, D.-X. Chen, J. Tang, A Method for Defensing Against Multi-source Sybil Attacks in VANET, Peer-to-Peer Networking and Applications 10(2)(2017) 305-314.

[11] T.B.M. de Sales, A. Perkusich, L.M. de Sales, H.O. de Almeida, G. Soares, M. de Sales, ASAP-V: A Privacy-preserving Authentication and Sybil Detection Protocol for VANETs, Information Sciences 372(2016) 208-224.

[12] B. Yu, C-Z. Xu, B Xiao, Detecting Sybil Attacks in VANETs, Journal of Parallel and Distributed Computing 73(6)(2013) 746-756.

[13] R. Hussain, H. Oh, On Secure and Privacy-aware Sybil Attack Detection in Vehicular Communications, Wireless Personal Communications 77(4)(2014) 2649-2673.

[14] J. Grover, V. Laxmi, M.S. Gaur, Sybil Attack Detection in VANET Using Neighbouring Vehicles, International Journal of Security and Networks 9(4)(2014) 222-233.

[15] M.K. Saggi, R. Kaur, Isolation of Sybil Attack in VANET Using Neighboring Information, in: 2015 IEEE International Advance Computing Conference (IACC), 2015.

[16] J. Grover, D. Kumar, M. Sargurunathan, M.S. Gaur, V. Laxmi, Performance Evaluation and Detection of Sybil Attacks in Vehicular Ad-Hoc Networks, in: International Conference on Network Security and Applications, 2010.

[17] A.S. Lal, R. Nair, Region Authority Based Collaborative Scheme to Detect Sybil Attacks in VANET, in: 2015 International Conference on Control Communication & Computing India (ICCC), 2015.

[18] M. Alimohammadi, A.A. Pouyan, Sybil Attack Detection Using a Low Cost Short Group Signature in VANET, in: 2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC), 2015.