Detection of Sybil attack in VANET

Dr.G. Anitha[1] *F. Stephen Raj*[2]

ABSTRACT

Vehicular Ad Hoc Network (VANET) is a kind of dynamic network in whichvehicular nodes can be connected or disconnected whenevernecessary. Vehicular Ad Hoc Networks (VANETs) have the potential to enable the next-generation Intelligence Transportation Systems (ITS). In ITS, data contributed from vehicles can build a spatiotemporal view of traffic statistics, which can consequently improve road safety and reduce slow traffic and jams. To preserve vehicles' privacy, they should use multiple pseudonyms instead of only one identity. The vehicular network is much exposed to the attacks which cause improper functioning of network. There is a possibility that a vehicle may exploit this abundance of pseudonyms and launch Sybil attacks by pretending to be multiple vehicles. These kinds of attacks possess false data, for example, to create fake congestion to affect traffic management data. To detect the Sybil attack, Road Side Units (RSU) behave as a proof for the vehicles'unspecified location. The several RSUs data contribution is received and fake trajectories of the vehicles can be solved by running the proof of work (PoW) Algorithm and Merged footprint and privacy-preserving algorithm and framed Hybrid Algorithm for the detection of corruptpseudonym methods. A valid solution should be provided to the upcoming RSU before it can obtain proof of location. Creation of multiple trajectories can be prevented by using the PoW in case of low-dense RSUs, and the performance of the Privacy-Preserving algorithm is more suitable when compared to footprint method high-dense RSUs.The speed of vehicles increases the performance of the footprint algorithm. The proposed algorithms are used to detect Sybil attack in an efficient way.

Index terms: ITS, VANET, Sybil attack, Proof of Work, Proof of Location

1. INTRODUCTION

Advancement in ad hoc wireless technology gives rise to the emergence of VANET. It acts like a crux for the Intelligent ITSs in the next generation, a chip that providesharmless roads. It is a networkwhich is formed by moving cars to create adynamic network, which helps to setup a connection between the vehicles to communicate with one another. Wi-Fi is the new technology used for the purpose of investigating the execution of VANET. The main aim of this application is to enable vehicles to contribute data and feedback, which is helpful for building a spatiotemporal view of traffic and jam statistics. It isrequired to preserve drivers' privacy, especially location privacy,while still verifying their identities in an anonymous manner. However, a pernicious vehicle may abuse this privacy protection to launch Sybil attack.The effects of a Sybil attack in VANETs can be dangerous. The consequence of a Sybil attack is in harmless applications such as avoiding accident and hazard warnings, which leads to biased results leading to car accidents. Advancement in ad hoc wireless technology gives rise to the emergence of VANET. It acts like a crux for the Intelligent ITSs in the next generation, a chip that providesharmless roads. It is a networkwhich is formed by moving cars to create adynamic network, which helps to setup a connection between the vehicles to communicate with one another. Wi-Fi is the new technology used for the purpose of investigating the execution of VANET. The main aim of this application is to enable vehicles to contribute data and feedback, which is

[1]Assistant Professor, Department of CS, CA & IT
Karpagam Academy of Higher Education

[2]Student, MCA, Department of CS, CA & IT
Karpagam Academy of Higher Education

helpful for building a spatiotemporal view of traffic and jam statistics. It isrequired to preserve drivers' privacy, especially location privacy,while still verifying their identities in an anonymous manner. However, a pernicious vehicle may abuse this privacy protection to launch Sybil attack.The effects of a Sybil attack in VANETs can be dangerous. The consequence of a Sybil attack is in harmless applications such as avoiding accident and hazard warnings, which leads to biased results leading to car accidents.

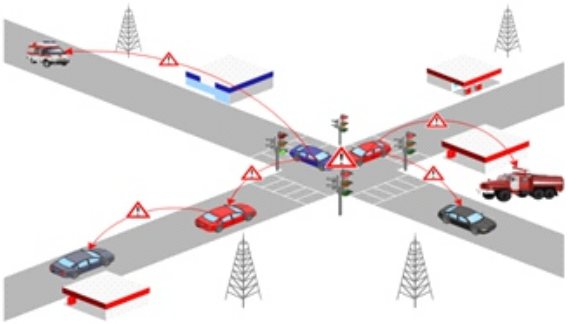

Figure 1: VANET Architecture

Vehicular Ad-hoc Network is classified into threeimportant system components, which are the AU, OBU and RSU:

- Smart vehicle:Vehicles are furnished with On-Board Unitin Vehicular Ad-hoc network. Itplays a vital roleinprocessing, interconnection and detectingthe location of the vehicles and navigating the routes.
- Application unit:The components of AUplay a major rolein alerting the vehicle driver and providing the safety of vehicles by sending an alert message. Itacts as anexplorer for creating an inter-communication network.
- On-Board unit:On-Board unit is used to constructan internalcommunication between the vehicles(V2V) and setup aninfrastructure to vehicles' communication (V2R).
- Road Side unit (RSU):RSU device is actuallyplacedata constant location, such as traffic signals. Itenlargesthe connection scope for the VANET by transmitting the messages within OBUs and transmitting important information to entities in its scope of transmission. This type of interaction with other RSUs, will runon safety applications and provide OBUs with internet connection.

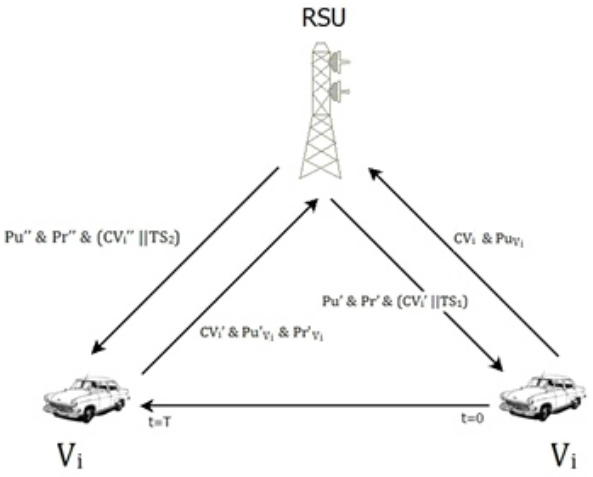

Figure 2: Key pair generation process in RSU

2. EXISTING WORK

Existing works for detecting Sybil attacks can bedividedinto three categories, namely identifying registration, position verification and trajectory-based approaches. The ultimate goal of these detection mechanisms is to ensure that each physical node is bound with a valid unique identity. However,finding the registration alone can'tforbid Sybil attacks, because a pernicious node may get collective identities by non-technical means such as stealing or even collision between vehicles. Position verification approaches are builtupon the aim that eachOBU be present in one location at a time. Detecting Sybil nodes by Global positioning System(GPS) is done by location information, which is provided by localization techniques. However, these schemes may fail due to the highly mobile context of vehicular networks. Trajectory-based approaches are based on the fact that individual vehicles move independently, and therefore they should travel along different routes. In [4], the vehicle obtains its trajectory by incorporating consecutive tags from RSUs, which it encounters. However, the scheme leads to RSU compromise attack. It means that all the RSUS

are compromised by compromising a single RSU in the network. Moreover, in case of rural areas (RSUs are not dense), attackers can create valid trajectories that look for different vehicles.

3.THE PROPOSED WORK

The proposed work on Sybil attack detection Scheme isbased on proofs of work and location. The main goal is that when a vehicle encounters an RSU,it will be authorized by a time-stamped tag which is a concatenation of time of appearance and anonymous location tag of that RSU.

As the vehicle keeps moving, it creates its trajectory by incorporating a set of consecutive authorized time-stamped tags that are chronologically chained to each other. That trajectory is used as an anonymous identity of the vehicle. Hence RSUs have the main authority to provide proof of location to vehicles. The scheme should withstand against RSU compromise attack. So we designed the trajectory so that not only one RSU is capable of creating trajectories for the vehicles. To achieve this, threshold signature is adopted so that each RSU is only able to generate a partial signature on a set of time-stamped tags. If a vehicle travels along a valid threshold number of RSUs, a standard signature representing a proof of location can be generated. Upon receiving an authorized message from an RSU, the vehicle should use it as a seed to solve a puzzle using a proof-of-work algorithm, similar to the one used in Bitcoin. The kernel idea of Proof of Work is to provide a proof to RSUs so they can ensure that the vehicle fix the puzzle correctly. Compared to Footprint [4], using PoW limits the ability of a pernicious vehicle to create multiple trajectories. To identify the Sybil trajectories, upon receiving an event from other vehicles, first of all the event manager has to perform a set of heuristics to construct a connected graph of Sybil nodes, after which it uses the maximum clique algorithm to detect all Sybil nodes in that graph. Our main contributions and the challenges can be summarized as follows:

Here I have used threshold signatures to defy RSU compromise attacks. The attacker needs to deal with an infeasible RSU to be able to create fake trajectories.

I have implemented the PoW algorithm to restrict the ability of a pernicious vehicle to create multiple fake trajectories, and more importantly, to reduce the detection time for Identifying the Sybil trajectories, which is animportant concern in traffic management applications.

I carefully analyzed the probabilistic nature of PoW-based scheme by examining the affecting parameters (e.g. travel time between two consecutive RSUs) experimentally, and then developed a mathematical model that could be used for adjusting these parameters so that the ability of a pernicious vehicle to create forged trajectories could be reduced significantly.

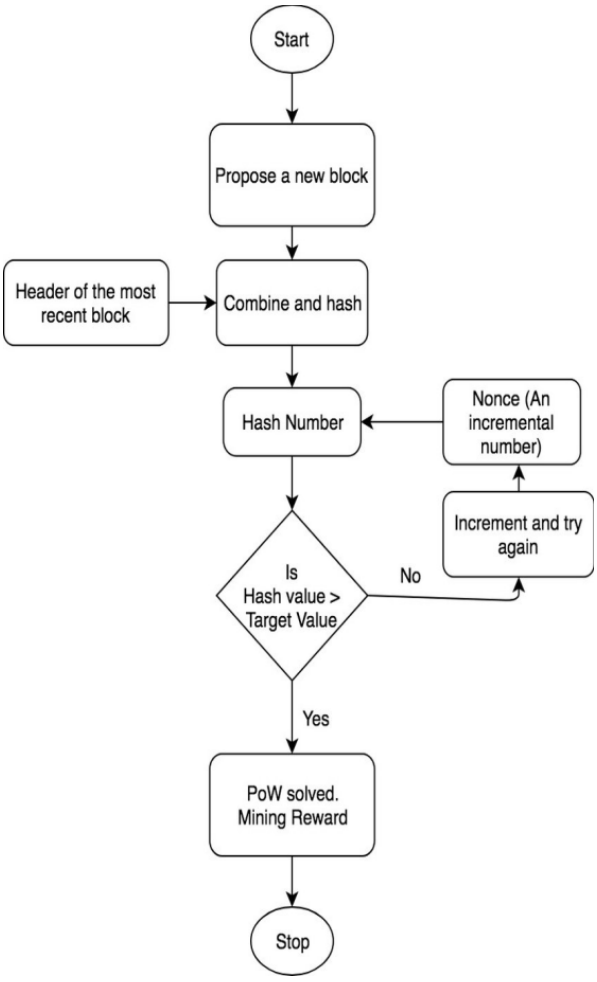

Figure 3: Proof of Work Flow Chart

By experiments, we have proved that using the PoW algorithm reduces the ability of a pernicious vehicle to maintain actual multiple trajectories continuously. Further simulations, analysis and practical experiments are conducted to assess the proposed work and compareit with the existing approach Footprint [4].The proposed work can successfully identify and preventSybil attacks in VANETs and perform tasks better than the Footprint does.

HYBRID ALGORITHM

It is designed by merging the privacy-preserving andfootprintalgorithm.This will improve the speed over the threshold footprint, otherwise privacy-preserving algorithmisimplemented. At the initial stage, it is implemented in the rural streets. Yearly, the pseudonyms are generated for each OBUs present in the network.Then pseudonyms are clustered in a one-way hash function. The hashed pseudonyms are grouped based on thechosen bits named “coarse-grained hash values”. The resultant groups are called “coarse-grained groups”, whichcan be hashed using a local key, kf. This local key is distributed to all the Road Side Unitsthat areconnected to the system, and the pseudonymsare disseminated to all the OBUs in VANETbased on the “fine-grained values”. Each OBU belongs to any “fine-grained group”. All Road Side Unitsin the network activate a link-tag concurrently. TA authenticates the link-tags, and transmit the same to the adjacent RSUs to identify themselvesin VANET.

The demonstration of the hybrid approach is shown infigure 4.It identifies the vehicles on the roadand can find the signals/information passed to each vehicle over the nearby Road Side Unit. The average speed of the vehicles will be examined by the RSUs. Different features such as speed and density on theroadcanvary as the speed increases, and the existing footprint approachis used to check whether there is a Sybil attack or not using the link-tags. Ifit isunique and there is no correlation and likenesses among them, and it shows that attacks are not found.

Onroad, the vehicle’s speedis evaluated using Hybrid algorithm. On the other hand, the Privacy-Preserving algorithm is executed to checkaSybil attack. The RSU receives the information by the message dissemination process in between the VANET nodes. The existing pseudonyms is clustered by the adjacent RSUusing the key kf.If “coarse-grained hash cluster” consistsof multiple pseudonyms, attack may be suspected and RSU sendsthe description to the DMV to check the presence of pseudonym in the same cluster and decides its attack status.If positive, there is sybil attack, or it is a fake alert message.

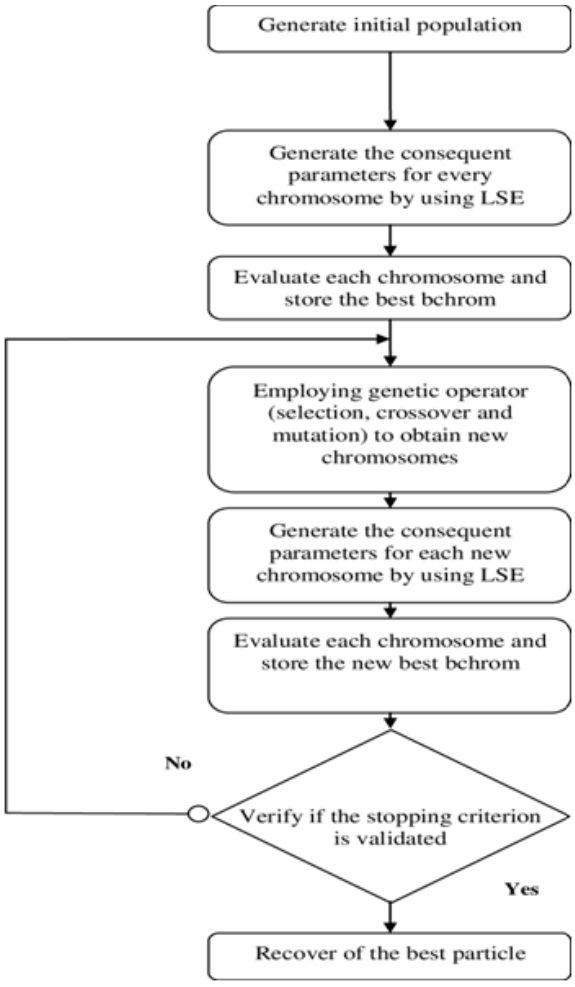

Figure 4: Flow Chart of Hybrid Algorithm

4. CONCLUSION

Sybil attacks can cause disastrous consequences in VANETS. In this paper, the proof of work and locations are the two different methods we have introduced for detecting

Sybil attacks. An anonymous trajectory of a vehicle is formed by obtaining consecutive proof of locations from multiple RSUs which it encounters. Instead of allowing only one RSU to issue authorized messages for vehicles, at least t RSUs are required for creating proof of location message using threshold signature to mitigate the RSU compromise attack. Footprint approach is used to identify Sybil attack;otherwise,Privacy-preserving method will detect the attack. Our experiments and evaluations have demonstrated that our scheme can identify Sybil attacks at ahigh rate and low false negative rate. However, the communication and computation overhead of the exchanged packets are acceptable.

6. REFERENCES

1. Jain, M. and R. Saxena. VANET: Security Attacks, Solution and Simulation. in Proceedings of the Second International Conference on Computational Intelligence and Informatics. 2018. Springer.
2. Rawat, A., S. Sharma, and R. Sushil, VANET: Security attacks and its possible solutions. Journal of Information and Operations Management, 2012. 3(1): p. 301.
3. Al-Sultan, S., et al., A comprehensive survey on vehicular Ad Hoc network. Journal of network and computer applications, 2014. 37: p. 380-392.
4. Aboobaker, A.K.K., Performance analysis of authentication protocols in vehicular ad hoc networks (VANET). Master of Science Thesis, Department of Mathematics, University of London, September, 2010. 2.
5. Patel, A. and P. Kaushik, Improving QoS of VANET Using Adaptive CCA Range and Transmission Range both for Intelligent Transportation System. Wireless Personal Communications, 2018. 100(3): p. 1063-1098.
6. F.-J. Wu and H. B. Lim, "Urbanmobilitysense: A user-centric participatory sensing system for transportation activity surveys," IEEE Sensors Journal, vol. 14, no. 12, pp. 4165–4174, 2014.
7. S. Hu, L. Su, H. Liu, H. Wang, and T. F. Abdelzaher, "Smartroad: Smartphone-based crowd sensing for traffic regulator detection and identification," ACM Transactions on Sensor Networks (TOSN), vol. 11, no. 4, p. 55, 2015.
8. K. Rabieh, M. M. Mahmoud, T. N. Guo, and M. Younis, "Cross-layer scheme for detecting large-scale colluding sybil attack in vanets," in 2015 IEEE International Conference on Communications (ICC). IEEE, 2015, pp. 7298–7303.
9. S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: Detecting sybil attacks in urban vehicular networks," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 6, pp. 1103–1114, 2012.
10. Z. MacHardy, A. Khan, K. Obana, and S. Iwashina, "V2x access technologies: Regulation, research, and remaining challenges," IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 1858–1877, 2018.
11. F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 2985–2996, 2015.
12. D. S. Reddy, V. Bapuji, A. Govardhan, and S. Sarma, "Sybil attack detection technique using session key certificate in vehicular ad hoc networks," in Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), 2017 International Conference on. IEEE, 2017, pp. 1–5.
13. T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "P2dapsybil attacks detection in vehicular ad hoc networks," IEEE journal on selected areas in communications, vol. 29, no. 3, pp. 582–594, 2011.
14. K. El Defrawy and G. Tsudik, "Privacy-preserving location-based ondemand routing in manets," IEEE journal on selected areas in communications, vol. 29, no. 10, pp. 1926–1934, 2011.
15. Y. Yao, B. Xiao, G. Wu, X. Liu, Z. Yu, K. Zhang, and X. Zhou, "Multichannel based sybil attack detection in vehicular ad hoc networks using rssi," IEEE Transactions on Mobile Computing, 2018.