IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024

DETECTING SYBIL ATTACK SUSING PROOFS OF WORK AND LOCATION INVANETS

[1]K SUPARNA, [2]S.RAVI TEJA

[1](Assistant Professor), MSC, DNR college(A) PG courses Bhimavaram

[2]MSC, scholar, DNR college(A) PG courses Bhimavaram

ABSTRACT

Vehicular Ad Hoc Networks(VANETs) has the potential to enable the next-generation Intelligent 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, vehicles should use multiple pseudonyms instead of only one identity. However, vehicles may exploit this abundance of pseudonyms and launch Sybil attacks by pretending to be multiple vehicles. Then, these Sybil (or fake) vehicles report falsedata, e.g., to create fake congestion or pollute traffic management data. In this paper, we propose a Sybil attack detection scheme using proofs of work and location. The idea is that each road side unit (RSU) issues a signed time-stamped tag as a proof forthe vehicle's anonymous location. Proofs sent from multiple consecutive RSUs isused to create vehicle trajectory which is used as vehicle anonymous identity. Also,one RSU is not able to issue trajectories for vehicles, rather the contributions ofseveral RSUs are needed. By this way, attackers need to compromise an infeasiblenumber of RSUs to create fake trajectories. Moreover, upon receiving the proof oflocation from an RSU, the vehicle should solve a computational puzzle by runningproof of work (PoW) algorithm. So, it should providea valid solution (proof ofwork) to the next RSU before it can obtain a proof of location. Using the PoW canprevent the vehicles from creating multiple trajectories in case of low-dense RSUs.Then, during any reported event, e.g., road congestion, the event manager uses amatching technique to identify the trajectories sent from Sybil vehicles. The schemedepends on the fact that the Sybil trajectories are bounded physically to one

ISSN 2347–3657

Volume 12, Issue 3, 2024

vehicle; therefore,their trajectories should overlap. Extensive experiments and simulation demonstrate that our scheme achieves high detection rate to Sybil attacks with low false negative and acceptable communication and computation overhea

1. INTRODUCTION

Over the last two decades, Vehicular Ad Hoc Networks (VANETs) have been emerging as a cornerstone to the next generation Intelligent Transportation Systems (ITSs), contributing to safer and more efficient roads. In VANETs, moving vehicles are enabled to communicate with each other via intervehicle communications as well as with road-side units (RSUs) in vicinity via RSU-to-vehicle communications. As a result, a wide spectrum of applications have been emerged as promising solutions [1] to enable new forms of ubiquitous traffic management applications that are not possible with our current traditional transportation system. The core idea of these applications is to enable vehicles to contribute with data and feedback to an event manager which can build a spatiotemporal view of the traffic state and also to extract important jam statistics [2]. These applications have the potential to contribute to safer and more efficient roads by enabling a wide range of applications such as pre-crash sensing and warning, traffic flow control, local hazard notification, and enhanced route guidance and navigation [3]

However, the aforementioned applications depend on information sent from participating vehicles. Therefore, it is required to preserve drivers privacy especially location privacy while still verifying their identities in an anonymous manner [4], [5]. A naive solution is to allow each vehicle to have a list of pseudonyms to be authenticated anonymously. However, a malicious vehicle may abuse this privacy protection to launch Sybil attack [6]. In Sybil attacks, a malicious vehicle uses its pseudonyms to pretend as multiple fake (or Sybil) nodes [7]. The consequences of a Sybil attack in VANETs can be disastrous. For example, a malicious vehicle can launch the attack to create an illusion of traffic congestion. Consequently, other vehicles will choose an alternative route and evacuate the road for the malicious vehicle. Another potential consequence of a Sybil attack is in safety-related applications such as collision avoidance and hazard warnings where a Sybil attack can lead to biased results that may result in car accidents [3]. Hence, it is of great importance to detect Sybil attacks in VANETs.

ISSN 2347–3657

Volume 12, Issue 3, 2024

Existing works of detecting Sybil attacks can be categorized into three categories, namely, identity registration, position verification and trajectory-based approaches. The ultimate goal of these detection mechanisms is to ensure each physical node is bounded with a valid unique identity. Firstly, identity registration approaches [7–9] require a dedicated vehicular public key infrastructure to certify individual vehicles with multiple pseudonyms to ensure each physical node is bounded with a valid unique identity. However, identity registration alone cannot prevent Sybil attacks, because a malicious node may get multiple identities by non-technical means such as stealing or even collusion between vehicles [10]. Secondly, position verification approaches depend on the fact that individual vehicle can present at only one location at a time. In [11], [3], localization techniques such as Global Positioning System (GPS) are used to provide location information of vehicles to detect Sybil nodes. However, these schemes fail due to the highly mobile context of vehicular networks [12]. Thirdly, trajectory-based approaches is 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 combining a consecutive tags from RSUs which it encounters. However, the scheme suffer RSU compromise attack in which if one RSU is compromised, a malicious vehicle can obtain infinite number of valid trajectories. Moreover, in case of rural areas (RSUs are not dense), attackers can create valid trajectories that look for different vehicles.

In this paper, we propose a novel Sybil attack detection scheme using proofs of work and location. The main idea is that when a vehicle encounters an RSU, the RSU should issue authorized 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 combining 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. Since RSUs have the main responsibility to issue proof of location to vehicles, the scheme should resist against RSU compromise attack so we design 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. Once a vehicle travels along a certain threshold number of RSUs, a standard

ISSN 2347–3657

Volume 12, Issue 3, 2024

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 [13]. The core idea of POW is to provide a proof to RSUs so they can ensure that the vehicle solved the puzzle correctly. Comparing to Footprint [4], using POW limits the ability of a malicious vehicles to create multiple trajectories.

To detect Sybil trajectories, upon receiving an event from other vehicles, the event manager first applies a set of heuristics to construct a connected graph of Sybil nodes, then it uses the maximum clique algorithm [14] to detect all Sybil nodes in
that graph.

Our main contributions and the challenges the paper aims to address can be summarized as follows:

We used threshold signatures to resist RSU compromise attacks. The attacker needs to compromise an infeasible number of RSUs to be able to create fake trajectories.

We used the POW algorithm to limit the ability of a malicious vehicle to create multiple forged trajectories, and more importantly, to reduce the detection time for detecting Sybil trajectories which is a critical concern in traffic management applications.

We 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 we developed a mathematical model that can be used for adjusting these parameters so that the ability of a malicious vehicle to create forged trajectories is reduced significantly.

By experiments, we prove that using the proof of work algorithm reduces the ability of a malicious vehicle to maintain actual multiple trajectories simultaneously. Further simulations, analysis, and practical experiments are conducted to evaluate the proposed scheme and compare it with the Footprint [4], the results indicate that the proposed scheme can successfully detect and defend against Sybil attacks in VANETs and more efficiently compared to the Footprint.

The rest of the paper is organized as follows. We describe the network and threat models in VANETs, followed by the design goal of our Sybil detection scheme in Section II. In Section III, we discuss preliminaries used by this research work. Then, our proposed scheme is presented in Section IV. In Section V, we show the selection of POW parameters values experimentally, and also we provide a mathematical proof of the experimental results. Detailed security and performance

ISSN 2347–3657

Volume 12, Issue 3, 2024

evaluations are provided in Section VI. We present the computation complexity analysis of our scheme in Section VII. Section VIII discusses the previous research work in Sybil detection in VANETs. Finally, we give concluding remarks in Section IX.

2.EXISTINGSYSTEM

anonymously. Meanwhile, if a particular node generates multiple signatures on the same message,theverifiercanrecognizethosesignatures.Asaresult,detectingduplicatedsignatures signed by the same vehicles can Zhou et al. [8] proposed a privacy-preserving scheme based on certificates to detectSybilnodes.Thedepartmentofmotorvehicle(DMV)representsthecertificateauthority, and is responsible for providing vehicles with a pool of pseudonyms to beused to hide the vehicle's unique identity. The pseudonyms associated with each vehicle are hashed to a common value. An RSU determines whether the pseudonyms come from the same poolby calculating the has hedvalues of the received pseudonyms. RSUs can detect Sybil nodes and then report such suspected vehicles toDMV.

To resist against RSU compromise, the paper suggests twolevelhash functions withdifferent keys (coarse-grained keys and fine-grained keys). RSU holds each validcoarse-grainedkeyonlyforashorttimewhichdoesnotknowwhetherthepseudonyms belong to one vehicle or not. If an RSU is compromised, the attacker only gets the coarse-grained hash key for the current time interval while DMV storesall keys and can detect Sybil nodes by two-level hashing. Although deploying trusted certificates is the most efficient approach that can completely eliminate Sybil attacks,it also violates both anonymity and location privacy of entities. Also, relying on acentralized authority to ensure each is assigned exactly one identity which becomes abottle neck in the large-scale network such as VANET.

In [30], Chen et al. proposed a group signature-based approach that can be used to enable amember in the group to authenticate himself/ herself eliminate Sybil attack. However, them alicious vehicle can launch Sybil attack, if he can generate different messages withsimilarmeaning.Recently,Reddyetal.[7]proposedacryptographicdigitalsignaturebasedmethodtoestablishthetrustrelationshipamongparticipatingentitie

DISADVANTAGES

- The system is no timplemented Hashing Keys in order to find Sybilattacks.

ISSN 2347–3657

Volume 12, Issue 3, 2024

The system is no timplemented attack resistance techniques in order to resist the Sybiland DDOS attacks

3. PROPOSEDSYSTEM

In this paper, we propose a novel Sybil attack detection scheme using proofs ofwork and location. The main idea is that when a vehicle encounters an RSU, theRSU should issue authorized 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 combining a set of consecutive authorizedtime-stampedtagsthatarechronologicallychainedtoeachother.Thattrajectoryis used as an anonymous identity of the vehicle. Since RSU shave the main responsibility to issue proof of location to vehicles, the scheme should resist against RSU compromise attack so we design 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. Once a vehicle travels along a certain threshold number of RSUs, a standard signature representing a proof of location can

begenerated. Upon receiving an authorized message from an RSU,the vehicles hould use it as a seed to solve a puzzle using a proof-of-work algorithm, similarto the one used in Bitcoin [13]. The core idea of PoW is to provide a proof toRSUs so they can ensure that the vehicle solved the puzzle correctly. Comparingto Footprint [4], using PoW limits the ability of a malicious vehicles to create multiple trajectories. To detect Sybil trajectories, upon receiving an event from other vehicles, the event manager first applies a set of heuristics to construct a connected graph of Sybil nodes, then it uses the maximum clique algorithm [14] to detect all Sybilnodes in that graph.

ADVANTAGES

- The system used threshold signatures to resist RSU compromise attacks. The attacker needs to compromise an infeasible number of RSUs to be able to create fake trajectories.
- The system used the PoW algorithm with Machine learning classifiers to limit theabilityofamaliciousvehicletocreatemultipleforgedtrajectories,andmoreimportantly, to reduce the detection time for detecting Sybil trajectories which is acritical concernin traffic management applications.
- The system carefully analyzed the probabilistic nature of PoW based scheme

ISSN 2347–3657

Volume 12, Issue 3, 2024

byexamining the affecting parameters (e.g travel time between two consecutive RSUs)experimentally, and then we developed a mathematical model that can be used for adjusting these parameters so that the ability of a malicious vehicle to create forged trajectories is reduced significantly.

- By experiments, we prove that using the actual multiple trajectories simultaneously. Further simulations, analysis, and practical experiments are conducted to evaluate the proposed scheme and compare it with the Footprint [4], the results indicate that the proposed scheme can successfully detect.

4.SCREEN SHOTS

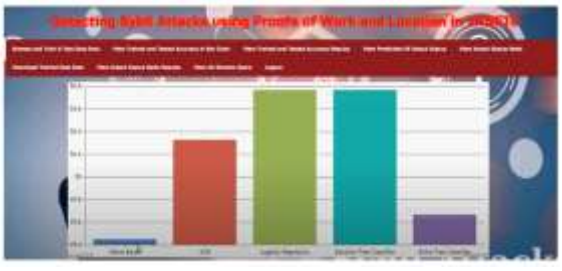
HOME PAGE

USER REGISTRATION

LOGIN SERVICE PROVIDER

DETECTING SYBIL ATTACKS USIG PROOFS

ACCURACY IN BAR CHART



ISSN 2347–3657

Volume 12, Issue 3, 2024

ACCURACY IN PIE CHART

5.CONCLUSION

Sybil attacks can cause disastrous consequences in VANETS. In this paper, we have introduced a novel approach for detecting Sybil attacks using proofs of work and location. An anonymous trajectory of a vehicle is formed by obtaining a consecutive proof of locations from multiple RSUs which Sybil attacks can cause disastrous consequences in VANETS. In this paper, we have introduced a Novel approach for detecting Sybilattack susing proofs of work and location. An anonymous trajectory of a vehicle is formed by obtaining a 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 a proof of location message using threshold signature to mitigate the RSU compromise attack. Also, the use of proof-of-work algorithm can limit the Ability of malicious vehicles to create forged trajectories. Our evaluations haved emonstrated that our scheme can detect Sybil attacks with high rate and low false negative rate. Moreover, the communication and computation overhead of the exchanged packet sare acceptable.

6.REFERENCE

[1] F.-J. Wu and H. B. Lim, “Urban mobility sense: A user-centric participatory sensing system for transportation activity surveys,” IEEE Sensors Journal, vol. 14, no. 12, pp. 4165–4174, 2014.

[2] 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.

[3] K. Rabieh, M. M. Mahmoud, T. N. Guo, and M. Younis, “Cross-layerscheme for detecting large-scale colluding sybil attack in vanets,” 2015 IEEE International Conference on Communications (ICC). IEEE,2015, pp. 7298–7303.

[4] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, “Footprint: Detectingsybil attacks in urban vehicular networks,” IEEE Transactions onParallel and Distributed Systems, vol. 23, no. 6, pp. 1103–1114, 2012.

[5] Z. MacHardy, A. Khan, K. Obana, and S. Iwashina, “V2x accesstechnologies:

ISSN 2347–3657

Volume 12, Issue 3, 2024

Regulation, research, and remaining challenges," IEEECommunications Surveys & Tutorials, vol. 20, no. 3, pp. 1858–1877,2018.

[6] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy reviewof vanets," IEEETransactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 2985–2996, 2015.

[7] 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.