IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12 , Iss 1, 2023

Advanced Sybil Attack Mitigation in VANETs via Proof of Work and Location-Based Techniques

DR.K.NAGESWARARAO, PROFESSOR
DEPARTMENT OF CSE
Sai Tirumala NVR Engineering College, Narasaraopet
Mail Id: nageswararaokapu@yahoo.com

ABSTRACT

Pharmaceutical medication development is a time-consuming and challenging process. Unexpected negative drug reactions that arise during the process may cause the entire drug development pipeline to be stopped or restarted. As a result, it is essential to predict the adverse effects of the medicine in advance of its design. In our Deep Side approach, we use context-related (gene expression) information along with the chemical structure to forecast ADRs, taking into account variables such as dosage, time interval, and cell line. By using GEX and CS as integrated features, the proposed MMNN model outperforms models that solely use chemical structure (CS) fingerprints in terms of accuracy. The claimed accuracy is remarkable considering that our objective is to forecast the adverse effects that are independent of the situation. Finally, the SMILES Conv model outperforms all other approaches by applying convolution to the SMILES representation of drug chemical structure.

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.

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 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 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. LITERATURE SURVEY

A user-centric participatory sensing system for transportation activity surveys,"

Participatory sensing (PS), an emerging sensing paradigm through organizing people and their mobile devices as sensors, is regarded as a promising solution to solve large-scale urban issues. PS has been implemented in many applications such as transportation, environmental monitoring, public health, etc. These applications are of high relevance for smart cities. Smart cities rely on the infrastructures established by government and industrial agencies to sense urban dynamics. PS can complement these infrastructures by involving "human sensors" and obtaining insights into people's activities. In this paper, the key features and challenges of PS are surveyed. A prototype PS platform is designed for efficient collection and management of smartphone sensing and survey data. A transport trip quality measurement system (TQMS) has been developed using this platform. Our experience to organize PS activities through a novel collaboration driven incentive mechanism is elucidated. A comprehensive real-world PS case study on TQMS including platform promotion, project collaboration, participant recruitment, activity organization has been successfully completed. This paper is concluded by discussing the potential future applications of the PS platform.

Smartphone-based crowd sensing for traffic regulator detection and identification,"

In this article we present SmartRoad, a crowd-sourced road sensing system that

detects and identifies traffic regulators, traffic lights, and stop signs, in particular. As an alternative to expensive road surveys, SmartRoad works on participatory sensing data collected from GPS sensors from in-vehicle smartphones. The resulting traffic regulator information can be used for many assisted-driving or navigation systems. In order to achieve accurate detection and identification under realistic and practical settings, SmartRoad automatically adapts to different application requirements by (i) intelligently choosing the most appropriate information representation and transmission schemes, and (ii) dynamically evolving its core detection and identification engines to effectively take advantage of any external ground truth information or manual label opportunity. We implemented SmartRoad on a vehicular smartphone test bed, and deployed it on 35 external volunteer users' vehicles for two months. Experiment results show that Smart Road can robustly, effectively, and efficiently carry out the detection and identification tasks.

"Cross-layer scheme for detecting large-scale colluding sybil attack in vanets," Vehicular networks are being progressively advocated for traffic and congestion management, accident prevention as well as enabling numerous location-based services. In vehicular networks, vehicles form platoons for improving operational efficiency and providing better traffic management thus resulting in optimized performance. However, platoons are vulnerable to notorious threats such as Sybil attacks wherein malicious users fabricate fictitious identities or impersonate those of legitimate nodes. In this paper, we model Sybil attacks in vehicular platoons using OMNET++, SUMO and Veins framework and evaluate their impact on performance. Further, a defense mechanism using hybrid key management in conjunction with witness based mechanisms is proposed. Evaluation shows that the proposed defense mechanism significantly limits the impact of Sybil attacks with minimal overhead. The proposed approach is lightweight in that public key based credentials are bootstrapped to set-up pairwise symmetric keys thus resulting in decreased overhead.

3. EXISTING SYSTEM

Zhou et al. [8] proposed a privacy-preserving scheme based on certificates to detect Sybil nodes. The department of motor vehicle (DMV) represents the certificate authority, and is responsible for providing vehicles with a pool of pseudonyms to be used 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 pool by calculating the hashed values of the received pseudonyms. RSUs can detect Sybil nodes and then report such suspected vehicles to DMV.

To resist against RSU compromise, the paper suggests twolevel hash functions with different keys (coarse-grained keys and fine-grained keys). RSU holds each valid coarse-grained key only for a short time which does not know whether the pseudonyms 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 stores all 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 a centralized authority to ensure each is assigned exactly one identity which becomes a bottleneck in the large-scale network such as VANETs.

In [30], Chen et al. proposed a group signature-based approach that can be used to enable a member in the group to authenticate himself/ herself anonymously. Meanwhile, if a particular node generates multiple signatures on the same message, the verifier can recognize those signatures. As a result, detecting duplicated signatures signed by the same vehicles can eliminate Sybil attack. However, the malicious vehicle can launch Sybil attack, if he can generate different messages with similar meaning. Recently, Reddy et al. [7] proposed a cryptographic digital signature based method to establish the trust relationship among participating entities.

The most relevant approach to our work is using trajectories of vehicles as its identities to ensure trust between participating nodes. In [32], RSUs broadcasts digital signatures with a timestamp to vehicles which are under its coverage. Vehicles store the RSUs signatures which they gathered in motion. However, since the time stamp is not issued for a dedicated vehicle, a malicious vehicle may claim its presence at certain RSU by merely eavesdropping such broadcasted timestamp on a wireless channel although it may have never been there at that time. In [4], Footprint has been introduced to detect Sybil attack. When a vehicle passes by an RSU, it obtains a signed message as proof of presence at this location at a particular time. A trajectory of a vehicle is a consecutive series of authorized messages collected by the vehicle as it keeps traveling. Sybil attack can be detected using the fact that the trajectories generated by an attacker are very similar. However, Footprint has some critical issues.

Disadvantages

The system is not implemented Hashing Keys in order to find Sybil attacks.

The system is not implemented attack resistance techniques in order to resist the Sybil and DDOS attacks.

4. PROPOSED SYSTEM

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 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.

Advantages

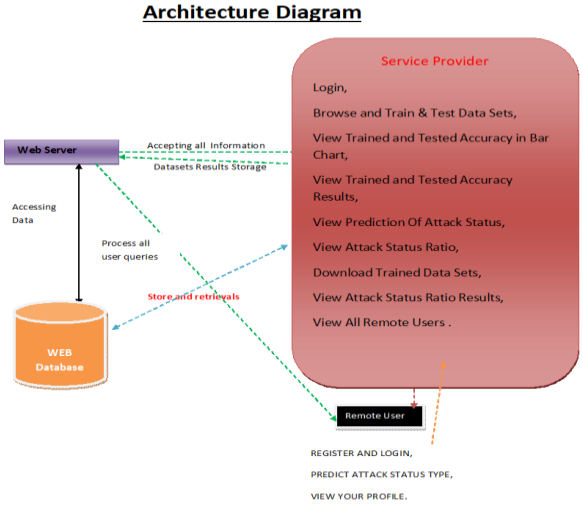
_ The system used threshold signatures to resist RSU compromise attacks. The attacker needs to compromise an infeasible number of RSUs to be able to create fake trajectories.

_ The system used the PoW algorithm with Machine learning classifiers to limit 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.

_ The system 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.

5. SYSTEM ARCHITECTURE



6. IMPLEMENTATION

MODULES

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Login, Browse and Train & Test Data Sets, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View Prediction Of Attack Status, View Attack Status Ratio, Download Trained Data Sets, View Attack Status Ratio Results, View All Remote Users.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

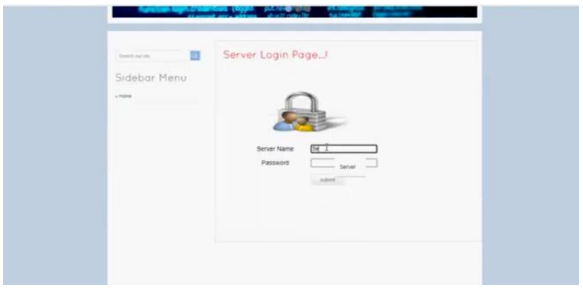
Remote User

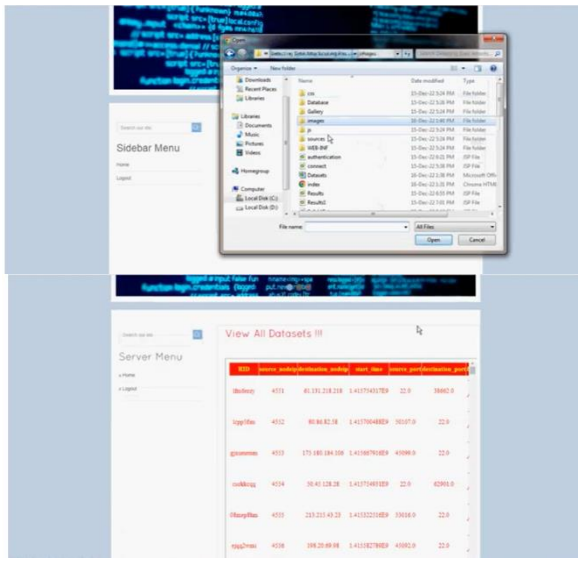
In this module, there are n numbers of users are present. User should register before

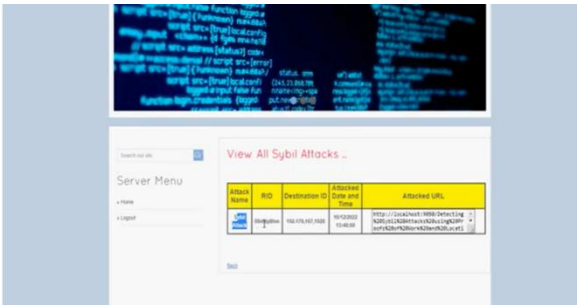
ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 12 , Iss 1, 2023

doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT ATTACK STATUS TYPE, VIEW YOUR PROFILE.

7. RESULTS







8. CONCLUSION AND FUTURE ENHANCEMENT

Sybil attacks could have disastrous consequences for VANETs. Here, we introduce a novel approach to Sybil attack detection based on proofs of work and location. To generate an anonymous vehicle trajectory, many RSUs provide sequential proof of location data. Sybil attacks have the potential to destroy VANETs. Here, we introduce a novel approach to Sybil attack detection based on proofs of work and location. The anonymous trajectory of a vehicle is constructed by obtaining sequential proof of location information from different RSUs that it encounters. Instead of allowing only one RSU to send approved messages for automobiles, at least t RSUs must use a threshold signature to deliver a proof of location message in order to thwart the RSU compromise attack. Furthermore, the proof-of-work approach may limit malicious vehicles' ability to generate fictitious trajectories. According to our experiments, our system has a low false negative rate and a high detection rate for Sybil assaults. Furthermore, there is a

reasonable processing and transmission overhead for the exchanged packets.

REFERENCES

[1] 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.

[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-layer scheme for detecting large-scale colluding sybil attack in vanets," in 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: Detecting sybil attacks in urban vehicular networks," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 6, pp. 1103–1114, 2012.

[5] 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.

[6] 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.

[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.

[8] 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.

[9] 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.

[10] 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.