International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

# Sybil Attack on Crowd Soured Mobile Mapping Services

**P. C. Zambare, Pornima Avaghade, Rohini Salunkhe, Ankita Shinde, Pooja Pilane**
Computer Engineering Department, NESGI, Pune, Maharashtra, India

**Article Info**
Volume 8, Issue 4
Page Number: 129-137

**Publication Issue :**
July-August-2021

**Article History**
Accepted : 10 July 2021
Published: 15 July2021

## ABSTRACT

Banks are giving flexible mobile applications to their client which is reliable, verified and secured however complex and vulnerable to a network problem. The problem in the current banking application is the unauthorized user can gain access to genuine user's accounts and perform unauthorized transactions. So as compared to the current banking application which is location free, we are developing a banking application utilizing location-based encryption which will be location dependent. User can easily perform transaction only if he/she is within TD (Toleration Distance) region. TD region is area of Toleration Distance (TD) where the users can perform the transaction. If the user goes out of TD region then the transaction will terminate automatically. We are also providing extra security by OTP and secret key.

Keywords- Online social networks, crowdsourcing, Sybil attack, location privacy, Mobile mapping, Mobile Computing, Spatial data collection, Web technologies

## I. INTRODUCTION

Over the years, it's very required high-quality security of knowledge and data resources has heightened and it'll easy to use. one among the best concerns in any enterprise environment is ineligible access to its data and multiple information platforms. An attacker targeting an enterprise environment would usually try and compromise one or more people password and physical security. password is that the most well-liked gateway to gaining access to several networks. when an attacker hacks the password of a legitimate user, often remotely, he gains access to the network. There are multiple malware attacks, involving both technical as well as non-technical implementation, which an attacker could published your username and 'steal' passwords. these include phishing, social engineering, social media accounts, password guessing, sniffing, eavesdropping, and man-in-the-middle attacks.

In the previous years, with the rapid development methods in network technology and upcoming techniques, the financial sector give the preference to computer networks extensively. But they're constantly being confronted with cyber-attacks. These financial sectors, especially the banking sectors mainly take the help of two sorts of security: computer security and network security. Computer Security is deemed to be an autonomous system offered with the assistance of Operating Systems (OS) and in-built hardware and software. Network

Security could be a broad term covering a mess of technologies, devices and processes. In simple words, it's a collection of rules and configurations that are designed so as to safeguard the integrity, confidentiality and accessibility of computer networks and data. this can be achieved using both software and hardware technologies so, We are designing a system for perfect security and reduce the hacking on online banking sector.

## II. RELATED WORK

Literature survey is that the most vital thanks to introduce your project idea or research. Before start developing, we'd like to check the previous papers of our domain which we are working and on the premise of study we will predict or generate the disadvantage and begin working with the reference of previous papers.

"Ghost Riders: Sybil Attacks on Crowdsourced Mobile Mapping Services Gang Wang , Bolun Wang, Tianyi Wang, Ana Nika, Haitao Zheng" within the paper of Real-time crowdsourced maps, like Waze provide timely updates on traffic, congestion, accidents, and points of interest. during this paper, we study lot of details view of a way to solve the dearth of powerful location authenticate, its take permission to creation of software-based Sybil devices that expose crowdsourced map systems to a range of security and privacy attacks. Our experiments show that one Sybil device with limited resources can cause havoc on Waze, reporting false congestion and accidents and automatically rerouting user traffic. most significantly, we explain the lot of techniques to making Sybil equipment at scale, creating also as updating armies of virtual vehicles capable of remotely tracking precise movements for big user populations while avoiding detection. To defend against Sybil devices, we propose also upcoming approaches which is supported co-location edges, authenticated records that attest to the one-time physical colocation of a pair of devices. Over time, co-location edges combine to make large proximity graphs that attest to physical interactions between devices, allowing scalable detection of virtual vehicles. We demonstrate the efficacy of this approach using large-scale simulations, and the way they will be wont to dramatically reduce the impact of the attacks. we've informed Waze/Google team of our research findings. Currently, we are in active collaboration with Waze team to boost the protection and privacy of their system [1].

In this paper, "Identification of Ghost Moving Detections in Automotive Scenarios with Deep Learning, Javier Martinez Garcia, Robert Prophet, Juan Carlos Victor Maria de Borbon y Borbon Fuentes Michel, Randolf Ebelt" We introduce a way to classify ghost moving detections in automotive radar sensors for advanced driver assistance systems. a completely connected network is employed to tell apart between real and false moving detections within the occupancy grid maps. By using this method structure, we gather the local Doppler information of knowledge, together with the spatial context of the encircling scenario which classify for detections. A proof-of-concept experiment shows promising results with data from a test drive in an urban scenario.[2].

In this paper, "Application of Geo-Location-Based Access Control in an Enterprise Environment Baba Meshach, Oluwafemi Osho and Anthony Sule" Unauthorized Access has been difficult to prevent or prevent within the previous few decades using username and password authentication only. For a private, data breach might just be an easy case of espionage or the loss of personal credentials, for an enterprise, this might mean the loss of billions of dollars. Preventing Unauthorized Access to Enterprise Systems employing a Location-based Logical Access Control proposes a framework that uses time and site in preventing and defending against data breaches. We use the platform of framework was Java with an

Eclipse IDE for the developments. The database was designed using MySQL and locations were collected using Google Maps API. Users registered at different locations during a university campus were unable to access another's account within the database because they were both outside the known location and tried to try to this at off work hours. Users were registered with username and password at specified locations. The users can easily login with our correct username and passwords by any location. it had been discovered that access to the database was only given when the username and password was correct and placement was same as at registered or as allowed by an administrator. The system was found to guard against unauthorized access arising from stolen login credentials and unauthorized remote logins from malicious users.[3].

In paper "The Sybil Attack and author is John R. Douceur" Large-scale peer-to-peer systems face security threats from faulty or hostile remote computing elements. To resist these threats, many such systems employ redundancy. However, if one faulty entity can present multiple identities, it can control a considerable fraction of the system, thereby undermining this redundancy. One approach to preventing these ìSybil attacksî is to own a trusted agency certify identities. This paper shows that, without a logically centralized authority, Sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities.[4].

This paper "Proximity-based Trust-advisor using E n coun ters for Mobile Societies and author Udayan Kumar, Gautam Thakur, Ahmed Helmy Many interactions between network users depend upon trust, which is becoming particularly important given the protection breaches within the Internet today. These problems are working with exploring by the various way in wireless mobile networks. during this paper we address the problem of trust advisory and establishment in mobile networks, with application to unplanned networks, including DTNs. We utilize encounters in mobile societies in novel ways, noticing that mobility provides opportunities to create proximity, location and similarity-based trust. Four new trust advisor filters are introduced - including encounter frequency, duration, behaviour vectors and behaviour matrices - and evaluated over an intensive set of real-world traces collected from a significant university. Two sets of statistical analyses are performed; the primary examines the underlying encounter relationships in mobile societies, and also the second evaluates DTN routing in mobile peer to-peer networks using trust and selfishness models. we discover that for the analysed trace, trust filters are stable in terms of growth with time (3 filters have near 90% overlap of users over a period of 9 weeks) and therefore the results produced by different filters are noticeably different. In our analysis for trust and selfishness model, our trust filters largely undo the effect of selfishness on the unreachability in an exceedingly network. Thus improving the connectivity in an exceedingly network with selfish nodes. We hope that our initial promising results open the door for further research on proximity-based trust.[5].

This paper "Attacks and Defences in Crowdsourced Mapping Services and Author Gang Wang† , Bolun Wang† , Tianyi Wang†‡, Ana Nika† , Bingzhe Liu†" Compared to traditional online maps, crowdsourced maps like Waze are unique in providing real-time updates on traffic, congestion, accidents and points of interest. during this paper, we explore the sensible impact of attacks against crowdsourced map systems, and develop robust defences against them. Our experiments show that one attacker with limited resources can cause havoc on Waze, reporting false congestion and accidents and automatically rerouting user traffic. We describe techniques to emulate Waze-enabled vehicles using lightweight scripts, and the way to use these "ghost riders" to compromise

user privacy by remotely tracking precise user movements while avoiding detection. one attacker can control groups of ghost riders, overwhelming data from legitimate users and magnifying the impact of attacks. As defense, we propose a brand-new approach supported co-location edges, authenticated records that attest to the one-time physical colocation of a pair of devices. Over time, co-location edges combine to make large proximity graphs, network that attest to physical interactions between devices. "Ghost-riders" cannot physically interact with real devices and may be detected using graph algorithms. We demonstrate the efficacy of this approach using large simulations, and discuss how they'll be wont to dramatically reduce the impact of attacks against crowdsourced mapping services.[6]

In this paper "Floating Car Data from Smartphones: What Google and Waze realize You and the way Hackers Can Control Traffic" Tobias Jeske in recent years, a trend of using real-time traffic data for navigation has developed. Google Navigation and Waze, for example, generate traffic data from movement profiles of smartphones. during this paper we tackle the question to which extent it's possible for Google and Waze to trace the smartphone and its owner. Furthermore, we show how wireless access points and smartphones acting like wireless access points will be located round the world. additionally, to the privacy issue, we examine whether the authenticity of traffic data may be guaranteed. We demonstrate in practice how hackers can take hold of navigation systems and, within the case of a large distribution of floating car data, can actively control the traffic flow. At the tip we present a practical protocol preventing such attacks and at the identical time preserving the user's privacy. The protocol has been implemented on different hardware platforms and benchmark results are given.[7]

In this paper "Know Thy Neighbor: Towards Optimal Mapping of Contacts to Social Graphs for DTN Routin Theus Hossmann, Thrasyvoulos Spyropoulos, and Franck Legendre" Delay Tolerant Networks (DTN) are networks of self-organizing wireless nodes, where end-to-end connectivity is intermittent. In these networks, forwarding decisions are generally made using locally collected knowledge about node behaviour (e.g., past contacts between nodes) to predict future contact opportunities. the employment of complex network analysis has been recently suggested to perform this prediction task and improve the performance of DTN routing. Contacts seen within the past are aggregated to a social graph, and a spread of metrics (e.g., centrality and similarity) or algorithms (e.g., community detection) are proposed to assess the utility of a node to deliver a content or bring it closer to the destination. during this paper, we argue that it's not such a lot the selection or sophistication of social metrics and algorithms that bears the foremost weight on performance, but rather the mapping from the mobility process generating contacts to the aggregated social graph. We first study two well-known DTN routing algorithms – SimBet and BubbleRap – that depend upon such complex network analysis, and show that their performance heavily depends on how the mapping (contact aggregation) is performed. what's more, for a spread of synthetic mobility models and real traces, we show that improved performances (up to an element of 4 in terms of delivery ratio) are consistently achieved for a comparatively narrow range of aggregation levels only, where the aggregated graph most closely reflects the underlying mobility structure. to the current end, we propose an internet algorithm that uses concepts from unsupervised learning and spectral graph theory to infer this "correct" graph structure; this algorithm allows each node to locally identify and fits the optimal operating point, and achieves good performance altogether scenarios considered [8]

In this paper "Ghost-Free High Dynamic Range Imaging via Moving Objects Detection and Extension, Benkang Zhang and Qin Liu and Takeshi IKENAGA†"

High dynamic range imaging (HDRI) techniques are proposed to synthesize high dynamic range (HDR) images from multi-exposure images. However, ghost artifacts may appear if images are synthesized directly when there are moving objects within the scene. This paper presents an algorithm to composite a HDR image from multi-exposure images without ghost artifacts. to get rid of the ghosts within the final image, the proposed algorithm firstly produces a 0-1 map supported a Markov Random Field (MRF) framework. The moving areas are detected and marked with 1. Then, moving areas are extended and utilized in the ultimate exposure fusion step. The marked pixels are assigned zero weights to stop ghost artifacts.[9]

In this paper "VISUAL SALIENCE AND STACK EXTENSION BASED GHOST REMOVAL FOR HIGH-DYNAMIC-RANGE IMAGING" Zijie Wang1,2, Qin Liu1,† , Takeshi Ikenaga2 High-dynamic-range imaging (HDRI) techniques are proposed to increase the dynamic range of captured images against sensor limitation. The key issue of multi-exposure fusion in HDRI is removing ghost artifacts caused by motion of moving objects and handheld cameras. This paper proposes a ghost-free HDRI algorithm supported visual salience and stack extension. to enhance the accuracy of ghost areas detection, visual salience based bilateral motion detection is introduced to live image differences. For exposure fusion, the proposed algorithm reduces brightness discontinuity and enhances details by stack extension, and rejects the knowledge of ghost areas to avoid artifacts via fusion masks. Experiment results show that the proposed algorithm can remove ghost artifacts accurately for both static and handheld cameras, remain robust to scenes with complex motion and keep low complexity over recent advances including patch-based method and rank minimization-based method by 20.4and 63.6[10]

## III. PROPOSED APPROACH

We develop new approaches for Mobile mapping system contains three main parts:

(i) the primary deals with the most components of mobile mapping systems. These include the digital imaging devices; the laser ranging and scanning devices; and therefore, the positioning (or geo-referencing) devices which are the principal building blocks that are getting used within the construction of such systems.

(ii) The second part will cover the system suppliers who integrate these different components and offer the resulting systems purchasable to users.

(iii) The third part covers a representative selection of service providers, but paying particular attention to the systems employed by the massive imaging and mapping organisations that have been mentioned above within the introduce

**System Diagram:**

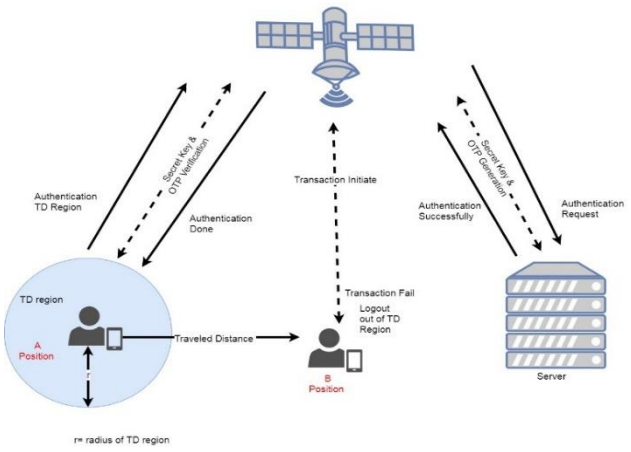


**Fig 1. System Architecture**

## IV. PROPOSED ALGORITHM

### I) Sybil Attack Detection:

Step 1: procedure DETECTION (locS, locR, s dataS, s dataR) for every snapshots
Step 2: status initialized to 0
Step 3: → Message validation
Step 4: if ts > τ then
Step 5: status = status + 1
Step 6: goto line 29
Step 7: end if
Step 8: → Sender verification
Step 9: dRS ← Cal Distance(locR, locS)
Step 10: φRS ← Cal Angle(locR, locS)
Step 11: if ObjectV erif ication(dRS, φRS, s dataR)! = VS then
Step 12: status = status + 1
Step 13: goto line 29
Step 14: end if
Step 15: → Surrounding objects verification
Step 16: SLi = ComputeOList(s dataS)
Step17:S
0
Li
= ComputeOList(s dataR)
Step 18:→ Compare S
0
Li
with SLi
Step 19: for each L0i ∈ L, rφ ≤ Li.φ
0 ≤ lφ do
Step 20: if ((Li.d
d
d ≤ Li.0
d
≤ L
i
.d
+
d
) & &
(Li.φ

φ ≤ Li.φ0
≤ Li
.φ
+

φ
) & &
(Li.0
type = Li.type)) then
Step 21: continue
Step 22: else
Step 23: status = status + 1
Step 24: return F ALSE
Step 25: end if
Step 26: end for
Step 27: → sybil attack detected
Step 28: if status == 3 then
Step 29: return F ALSE
Step 30: end if
Step 31: → need more checking for possible sybil attack
Step 32: if status < 3 then
Step33: goto line 2 with another snapshot
Step 34: end if
Step 35: → sybil attack not detected
Step 36: return T RUE
Step37: end procedure

## V. EXPERIMENTAL RESULT

### A) SYBIL ATTACK DETECTION SCHEME:

Our proposed scheme consists of three phases to detect sybil attacks: i) message validation; ii) sender verification; iii) surrounding objects verification.

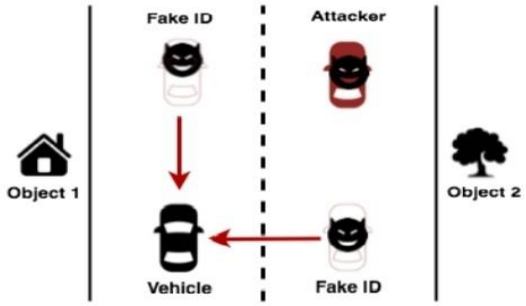


**Fig 2. Scenario of Sybil Attack**

The proposed Sybil attack detection scheme is discussed very well as follows. The vehicle VR receiving a message M from the source vehicle VS executes the algorithm for detecting sybil attack as shown in Algorithm 1. The message M contains three snapshots sn information including gps information loc and sensor data s data from the source vehicle VS.

To begin the message validation process, VR first checks if the timestamps of the message M and snapshots sn are within the edge τ and valid. the method of message validation is illustrated. If M is valid, then it proceeds to the sender

verification that verifies if the sender vehicle actually exists at the claimed location.

In order to verify the sender, the space dRS and therefore the angle φRS between VR and VS are calculated and people are compared with the situation information sent by VS to test if the sender vehicle is really located at the claimed location. Note that the angle and also the distance are calculated from the middle points of every vehicle/object. If this verification fails, then it increases the worth of the status by one, which is initially set to zero at the start. The process of the sender verification is illustrated. Once the placement of the sender vehicle is verified, then its surrounding objects are verified because the encircling objects near VS should even be captured by VR. the method of surrounding object verification is illustrated. Note that some objects/vehicles may not be detected as they will be blocked by other objects/vehicles.

To address this issue caused by no line of sight, multiple snapshots of sensor data are taken so even if some objects/vehicles are missed in one snapshot, they will be detected in other snapshots. That being said, multiple snapshots taken at different times are accustomed determine a sybil attack.It is worth noting that we also assume that the all clocks in vehicles are synchronized and VR and VS

have the sensor data that were generated at the identical time Ts.

Before verifying the surround objects, the method generates two objects lists from each snapshot: SLi generated with s dataS and S 0 Li generated with s dataR, respectively.

Note that the thing list contains the locality information including distance, angle, and therefore the object type. Once the item lists are generated, then the space and also the angle of the identical object are evaluated if they're within the error boundary. Also, the item variety of the article is compared if they're the identical form of the thing. This process repeats for the nearby objects within the object lists. After the encompassing object verification process, the status value is evaluated to see if a sybil attack is detected. If status == 3, it means all three snapshots fails the verification, hence a sybil attack is detected.

If status < 3

## B) SYBIL ATTACK DEFENSE: SOLUTIONS AND SCHEMES:

Recently, interest and efforts for defending against malicious attacks in social networks using reliable solutions and schemes have increased Several proposed schemes strive to attenuate Sybil attacks in an OSN by utilizing the properties of the OSN's structure. Unlike the normal solutions discussed within the previous section, these existing solutions and schemes don't require central trusted identities. Instead, they solely depend upon the trust personified

within the existing social relationships that occur between the users of the OSN. Most literature on existing sybil defense mechanisms show that these mechanisms are in early stages of development.

Therefore, most of those researchers describe new algorithms in their papers; however, they are doing not present a technique by which all the proposed schemes can detect the occurrence of Sybil attacks.

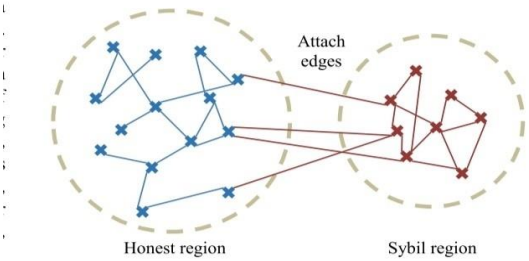


**Fig 3 Legitimate and Sybil regions.**

during this section, we offer an summary of various Sybil schemes that are utilized by researchers to execute various Sybil detection and prevention algorithms and tools.

In general, the Sybil schemes are divided into four main categories: Graph-based schemes, machine-learning-based schemes, manual verification and Prevention approaches. Graph-based (also called network-based schemes are further divided into subcategories: Sybil detection and Sybil tolerance.

## VI. APPLICATION

1. Aerial mobile mapping
2. Emergency response planning
3. Internet applications
4. Road mapping and highway facility management
5. Digital Twins applications

## VII. CONCLUSION

In this paper, using this system user can able to do the secure transaction from mobile with the help of Geography location and anti-spoof GPS. In case of physical attack, our system creates a virtual environment with extra key bit in password.

## VIII. REFERENCES

[1]. C Ngo, Y Demchencko, and C de Laat, "Multi-tenant attribute-based access control for cloud infrastructure services," Journal of Information Security and Applications, 2015.

[2]. J Brassil, P K Manadhata, and R Netravali, "Traffic signature-based mobile device location authentication," IEEE Transactions on Mobile Computing, , vol. 13, no. 9, pp. 2156-2169, 2014.

[3]. Olayemi M. Olaniyi, Folorunso A. Taliha , Aliyu Ahmed, and Olugbenga Joseph, "Design of Secure Electronic Voting System Using Fingerprint Biometrics and CryptoWatermarking Approach," International Journal of Information Engineering and Electronic Business(IJIEEB), pp. 9-17, September 2016.

[4]. Roselin Chirchi Vanaja and Laxman. M Waghmare, "Iris Biometric Authentication used for Security Systems," Iinternational Journal of Image, Graphics and Signal Processing, pp. 54-60, August 2014.

[5]. F. Roos, M. Sadeghi, J. Bechter, N. Appenrodt, J. Dickmann, and C. Waldschmidt, “Ghost Target Identification by Analysis of the Doppler Distribution in Automotive Scenarios,” 18th International Radar Symposium, Prague, Czech Republic, Jun. 2017.

[6]. R. Prophet, J. Martinez, J. C. Fuentes, R. Ebelt and M.Vossiek, “Instantaneous Ghost Detection Identification in Automotive Scenarios”,

submitted to IEEE Radar Conference, Boston, MA, USA, Apr. 2019.

[7]. L.C. Chen, G. Papandreou, F. Schroff and H. Adam, "Rethinking Atrous Convolution for Semantic Image Segmentation," arXiv 1706.05587, 2017.

[8]. M. Oquab, L. Bottou, I. Laptev and J. Sivic, "Is object localization for free? - Weakly-supervised learning with convolutional neural networks," 2015 IEEE Conf. on Computer Vision and Pattern Recognition, Boston, MA, USA, 2015, pp. 685-694.

[9]. J. Long, E. Shelhamer, and T. Darrell, "Fully convolutional networks forsemantic segmentation," CVPR, pp. 3431-3440, 2015.

[10]. J. Martinez and M. Vossiek "Deep Learning-Based Segmentation for the Extraction of Micro-Doppler Signatures," in procc. of the European Microwave Week (EuRAD), Madrid, Spain, Sept. 2018.

[11]. K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," Int. Conf. on Learning Representations, pp. 1-13, 2015.

[12]. B. Wang, L. Zhang, and N. Z. Gong, "SybilSCAR: Sybil detection in online social networks via local rule based propagation," in Proc. INFOCOM, 2017.

**Cite this article as :**

P. C. Zambare, Pornima Avaghade, Rohini Salunkhe, Ankita Shinde, Pooja Pilane, "Sybil Attack on Crowd Soured Mobile Mapping Services", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 4, pp. 129-137, July-August 2021.

Journal URL : https://ijsrset.com/IJSRSET184105