IJCSI International Journal of Computer Science Issues, Volume 15, Issue 6, November 2018
ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784
www.IJCSI.org https://doi.org/10.5281/zenodo.2544625

Sybil Attacks and Defenses in Internet of Things and Mobile Social Networks

Ali Alharbi[1], Mohamed Zohdy[1], Debatosh Debnath[1], Richard Olawoyin[1] and George Corser[2]

[1] Computer Science, Oakland University
Auburn Hills, Michigan 48307, USA

[2] Computer Science, Saginaw Valley State University
Saginaw, USA

Abstract

Sybil attacks present a unique threat in the context of Mobile Social Networks and the Internet of Things. Existing research activity in this field focuses on developing novel detection techniques or improving existing ones, but there is a paucity of knowledge about the current types of Sybil attacks and their countermeasures. The purpose of this paper is to explore the different types of Sybil attacks and potential countermeasures. An extensive literature review is conducted to analyze Sybil attacks and classify the defense methods and techniques. The findings show that the common Sybil attacks in MSN and IoT can be categorized into three orthogonal dimensions that represent distinct attack characteristics: direct and indirect communication attacks; fabricated and stolen identity attacks; and simultaneous and non-simultaneous attacks. In Wireless Sensor Networks (WSNs), Sybil attacks can be categorized further into four types depending on the protocols that they target: routing attacks, distribution storage attacks, data aggregation attacks, and resource allocation attacks. The defense mechanisms fall into four broad categories: graph-based methods, Machine Learning techniques, prevention methods, and manual verification methods.

Keywords: *countermeasures, graph-based methods; Internet of Things; machine learning; manual verification; Mobile Social Networks; prevention, Sybil attacks*

1. Introduction

A. Sybil Attack and Its Importance

The recent advances in information technology provide important benefits and opportunities associated with distributed computing systems and networks such as autonomy, data sharing, and availability. However, these benefits come with increased security risks that limit the usage of distributed systems. One of the most prominent security risks is Sybil attack in which an adversary generates multiple fake identities to control legitimate network nodes. In particular, a Sybil attack involves subverting the identities of nodes by creating pseudonymous identities for facilitating malicious access to a network [1].

All identity attacks present a significant security risk in distributed networks and a major challenge in the context of the Internet of Things (IoT) and Mobile Social Networks. The main problem in Sybil attacks is the challenge of distinguishing the attackers from normal users [2]. While MSNs provide an efficient environment for users to access, share, and distribute data, the lack of a sufficient protective infrastructure makes these networks vulnerable to identity attacks. In MSNs, Sybil attacks present a major challenge as they often entail the creation of a relationship between a malicious user and an honest user [3]. The attackers can spread spam in MSNs, mislead popularity, or breach user privacy [4].

B. How Sybil Attacks Work

Although Sybil attacks are diverse, they involve a similar attack strategy aimed at undermining a system. The core of the Sybil attack anatomy is the creation of multiple identities and influencing the working systems. An attacker intending to launch Sybil attack must create links to the honest nodes in a network. The next step is to create fake identities. The fabricated identities look like the normal nodes. An adversary can fabricate node identities using two options: using real identities to broadcast its presence to other nodes or using virtual identities to interact with the attackers' real IDs [5]. When using real identity approach, an adversary can use a single physical device to create many real identities to broadcast it to the network nodes. The detection of such an attack requires additional resources such as battery power and special knowledge of the broadcasting protocols [5]. The limitation of these resources makes it difficult to detect and prevent attacks using real IDs. On the other hand, virtual identities interact with an attacker's real IDs only; these identities do not interact with the network nodes because they do not need to broadcast themselves to facilitate communications [5]. Figure 1 illustrates the interactions between attack identities (real IDs and virtual IDs), and honest nodes.

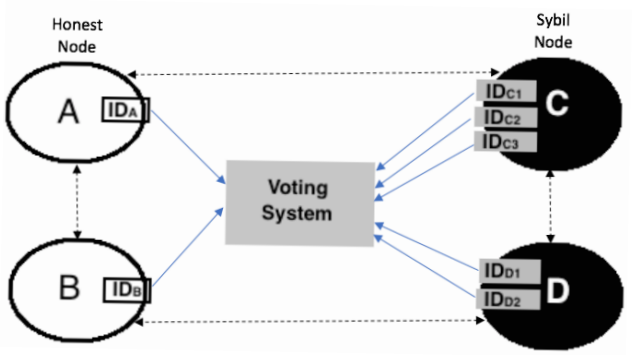

Figure 1. Real identities and Virtual identities in a Sybil nodes in voting system.

C. *Impact of Sybil Attacks*

Sybil attacks have essential implications in IoT environments and MSNs. In IoT, Sybil attack can affect the entire network of 'things' or a portion of the system domains. The attack can affect the performance of IoT by creating additional overhead as well as present privacy and security threats to users and connected devices [2]. In IoT environments, Sybil attacks have the potential to disseminate spam using fake identities or compromise IoT effectiveness by abusing pseudo-identities [2]. In MSNs, attackers can violate user privacy, breach information security and spread spam or mislead popularity [4].

D. *Organization of the Paper*

The paper is organized as follows; Section 1 is an introduction to Sybil attacks focusing on what the attack involves, how it works, and its impact. Section 2 entails a description of different types of Sybil attacks with a detailed comparison. Section 3 covers the common defense mechanisms and their comparisons. Section 4 explores future work on the topic and Section 5 concludes the research work.

2. Sybil Attacks

E. *Types of Sybil Attacks*

In [6], the authors present a taxonomy of Sybil attacks based on six characteristics representing attacker capabilities or dimensions: insider or outsider, selfish or malicious, directed or in-directed, simultaneous or gradual, busy or idle, and discarded or retained. The overall idea is that the categorization of Sybil attacks in terms of the impact of severity depends on the attack capabilities. Inside attackers tend to have the enormous impact toward networks because the adversary has connections to legitimate identity, which increases the vulnerability to fake identities [6]. In direct communication, a genuine node sends radio messages to a Sybil node (Figure 2); M represents the malicious node, and S Sybil identifies of M. In fabricated identities, the adversary creates arbitrary identities (Figure 3).

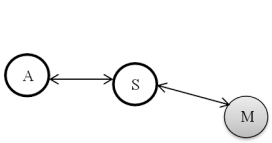

Figure 2. Direct communication [8]

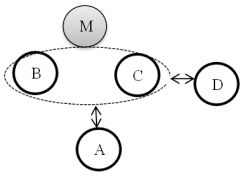

Figure 3. Fabricated identities [8]

In [7] [8] [26], the authors describe six main types of Sybil attacks on distributed network protocols: routing attacks, attacks targeting voting and reputation systems, resource allocation, distributed storage, and data aggregation attacks, and misbehavior detection.

1) Routing This type of attack involves distortion of routing protocols, especially in *ad hoc* networks. The attack may involve separate multiple paths going through Sybil nodes or involve geographic routing in which sensor nodes route data into the base station [7]. Generally, the current routing protocols are mostly designed to extend their limited node capabilities, which introduce security vulnerabilities. For example, WSNs cannot use the security resources available to the conventional network. Sybil attacks present a unique risk in these routing protocols as forging multiple identities can undermine mapping between identities.

2) Distributed storage In this type of attack, an adversary may store data on false identities created by malicious nodes. The attacker can compromise file storage systems and trick users to store data in multiple Sybil identities of a network node [7]. This involves fragmenting of replicating data across multiple Sybil nodes under the same malicious node. Alternatively, Sybil attacks can involve decreasing the effectiveness of distributed storage.

3) Data aggregation In data aggregation attacks, the adversary can assume multiple identities and alter aggregation readings in sensor networks as a strategy to conserve energy. When a malicious nodes report incorrect readings, they cannot affect the computed aggregate, but a Sybil attack contributes to significantly to the aggregate as a single malicious node can generate multiple fake identities [26].

4) Voting and reputation systems An adversary can target a voting scheme by updating reputation scores using fake identities [7]. Sybil attacks target reputation systems including eBay because these systems allow spammers to use multiple accounts on free email systems. For example, an attacker can target Google Page Rank rating by linking search terms to create fake ratings. Sybil attackers can also manipulate computing systems that use voting to authenticate correct answers to accept false solutions.

5) Resource allocation A malicious node based on Sybil attack can obtain disproportionate resource allocation and cause Denial of Service (DoS) by denying legitimate access to network resources [7]. This type of attack is common in networks where resources are assigned depending on the number of nodes [26]. A Sybil attack on such a network can allow malicious nodes to obtain a disproportionate share of computing resources while denying service to the legitimate nodes.

6) Misbehavior detection attacks In this type of attack, an adversary creates multiple Sybil nodes to spread false alarm. In

a misbehavior detection system, this kind of adversarial activity results to false positives. The intention of such an attack is to affect the performance of such a system and reduce its detection accuracy [26].

In [2], the authors categorize Sybil attacks in the IoT based on the target IoT domains. The first category is the SA-1 Sybil attackers, which entails tight Sybil nodes connected to other nodes to create a community of anomalous identities. This category of attackers exists in the sensing and social domains of the IoT, which means it can be common in an online voting system or mobile sensing system [2]. The capability of the SA-1 attacker to establish social connections with legitimate nodes is weak, which limits the potential impact of the attack.

The second category is the SA-2 Sybil attack, which exists in the social domain of IoT. This attack relies on the ability to create social connections among Sybil identities and normal users [2]. SA-2 attackers have the capacity to mimic normal users with a large attack surface. The primary goal of this type of attack is to disseminate malware and spam, to manipulate reputation systems, and to spread spam [2].

The third category of is the SA-3, that target the mobile networks such as MSN. The primary goal of this attack is similar to SA-2, but the impact of the former is limited within a local area. This is especially important considering that mobile networks cannot allow long-term connections given their intermitted connection characteristics [2].

F. Comparison of Sybil Attacks

TABLE I. COMPARISON OF SYBIL ATTACK TYPES

Types of Attacks/Target Protocols and Services	**Description of Attacks**
Routing	Can invalidate multipath routing protocols by directing traffic via malicious nodes connected to multiple Sybil nodes
Distributed storage	These attacks aim at replicating or disintegrating data across multiple Sybil nodes or manipulating the malicious nodes to store data
Data aggregation	Malicious nodes can alter or modify aggregate data reading
Voting/reputation systems	Sybil attacks can generate fake votes and affect the ranking mechanisms in reputation systems
Resource allocation	Malicious nodes can deny legitimate nodes from accessing computing resources
Misbehavior detection	Multiple Sybil nodes result to false alarms that disrupt detection systems

3. Sybil Attack Defenses

G. Common Defense Schemes and Mechanisms

While Sybil attacks present a significant problem, there is currently no universally accepted technique for defending against these attacks. In [9], the authors propose a classification scheme of Sybil defense schemes. The scheme categorizes defense mechanisms into four broad categories; graph-based methods, machine learning methods, manual verification methods, and prevention approaches [9].

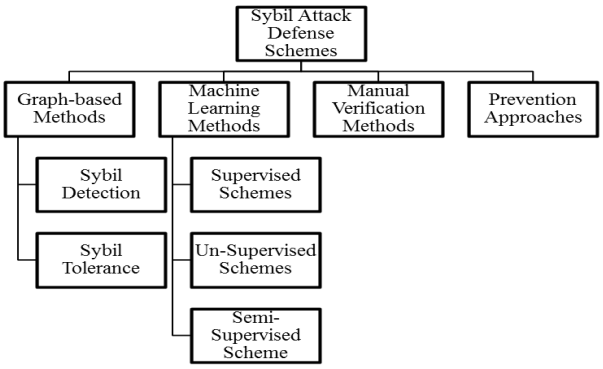

Figure 4. Classification scheme of Sybil defense methods and techniques Adopted from [9].

1) Graph-based (network) Sybil detection (GSD) methods The graph-based schemes rely on social network information to represent the dependency among objects. These methods fall into two categories: Sybil detection techniques based on the concept of graph random walk and mix time, and Sybil tolerance methods, which limit the effects of Sybil attack edges [9]. In [11], the researchers propose a distributed technique for detecting Sybil attacks in MANETs. Each node in the network monitors traffic as a mechanism for detecting signs of Sybil attacks. The evaluation shows an accuracy of 80% and error rate of 10%, which shows the feasibility of using the method to protect against Sybil attacks in mobile networks. In [12], MobID is presented, a method that protects portable devices against Sybil attacks. The evaluation of the technique shows that MobID limits interactions between devices and attackers. Similarly, in [13], the authors describe graph-based Sybil detection methods using decision trees and other behavioral analytics. The authors conclude that techniques for refining node identification in MSNs can address the current problem with Sybil attacks. The authors in [14], proposed a lightweight scheme for the detection of Sybil attackers in MANETs using Received Signal Strength (RSS)-based localization to distinguish between Sybil and legitimate identities. Simulation experiments using the proposed approach show that it can detect Sybil identities in mobile environments, which indicates the feasibility of the proposed detection scheme in *ad hoc* network environments. In [15], the researchers present a mechanism for detecting and eliminating Sybil nodes in MSNs by facilitating cooperation by mobile terminals and servers. The proposed mechanism exploits the social-based routing in MSNs to defend against Sybil attackers. Chinchore et al. [16] described a graph-based technique for detecting Sybil attacks, which relies on accurate identification of the behavior of fake nodes from honest nodes on MSNs. The method helps to identify the behavior of users by the starting and ending time of connections. Gu et al. [17] propose another approach to Sybil attack detection using driving patterns in vehicular networks. The method detects erotic Sybil driving patterns. Simulation experiments showed that the detection method has high detection accuracy of 90% and low error rate of 10%.

2) Machine-learning defense methods Machine learning methods fall into three categories: supervised, un-supervised,

and the semi-supervised. Supervised methods use regression models, SVM, and decision tree models. Unsupervised methods use fuzzy logic, Markov models, and clustering methods, while semi-supervised methods use sets of data to improve the quality of learning [9]. In [4], the authors presented a semi-supervised learning technique that uses Hidden Markov Model to detect malicious mobile users and Sybil attackers. Evaluations of the proposed method show its feasibility in detecting Sybil attacks in MSNs. Gu et al. [18], propose a Sybil attack detection method in vehicular networks that uses SVM. In this method [18], the authors evaluate driving patterns to distinguish malicious nodes from the normal ones. Simulation results showed that the proposed method could achieve high detection rate and low error rate in a dynamic environment such as MSNs. Chinchore [19] described a novel graph-based data mining model for identification of Sybil nodes using classification and regression schemes. The proposed scheme identifies dependencies using attributes such as connection duration. In [20], the authors describe a technique for detecting Sybil attacks in vehicular networks using k-Nearest Neighbor (kNN) classification algorithm. The researchers used the kNN algorithm to distinguish virtual nodes from benign nodes. The simulation experiments demonstrated the feasibility of the proposed machine-learning algorithm in terms of detection rate and error control.

H. Comparison of Sybil Defense Methods

3) Manual verification methods Manual verification relies on users to improve privacy and security through user verification. In social networks, this may include asking users to report malicious content [9].

4) Prevention methods Prevention approaches represent the conventional and traditional approach to mitigating Sybil attacks using trusted authorities or connecting identities to trusted resources. That is, the use provides trusted and verified identities. Some of the common approaches include the use of crypto-puzzles (CAPTCHA) for users to access services. In [7], the authors various techniques for preventing Sybil attacks including using trusted certification authority (CA), resource testing, recurring costs, privilege attenuation, incentive-based detection, and location verification. In [10], the authors present a robust method for defending against Sybil attacks in VANETs using timestamp series, a trusted certification scheme.

In [24], the authors describe other Sybil defenses using various approaches such as indirect radio communication, registration, code attestation, and key pre-distribution. In [25], the authors describe Event-Based Reputation System for defending against Sybil attacks, which can safeguard voting systems and reputations systems against potential attacks.

TABLE II. COMPARISON OF SYBIL DEFENSE METHODS

Classification Schemes	**Categories of Classification Scheme**	**General Features and Characteristics**	**Advantages**	**Disadvantages**	**Examples of defense methods/schemes proposed in literature**
Graph-based Sybil Detection Schemes	***Sybil Detection***	Uses the concept of graph random walk and mixing time Assumes that neighbors share secret symmetric keys in a social graph	Often a decentralized approach No barriers	Significant overhead Scalability issues Changes in network infrastructure can invalidate node identities	SybilGuard [21] SybilLimit [22] Others: [11], [14], [15], [16]
	Sybil Tolerance	They limit the impact of Sybil attack edges	Decentralized	Scalability issues Performance overhead in network	MobID [12] [13]
Machine Learning Schemes	***Supervised***	Uses labeled training dataset Relies on feature engineering using domain knowledge Uses regression models, SVM, decision tree models, and naïve Bayes	Useful when working with massive data amounts Better detection rate	Highly dependent on domain knowledge Training data on large scale is problematic Requires a lot of data (data shortage problem) False alarm rate due to noise in training dataset	[18]

	Un-supervised	Do not require training data Uses clustering and latent variables methods	Can uncover hidden structures More resistance to previously unknown attacks	False positives (error rate)	[19]
	Semi-supervised	Human experts label a portion of the data during the acquisition stage Uses labeled and unlabeled data to improve learning quality	Flexibility to integrate labeled and unlabeled data Requires small quantity of training data	Problem of handling mixed datasets	[4], [23]
Prevention Schemes	***Prevention***	Rely on trusted central authorities to prevent attacks	Controls entities that join the system	Requires online trusted authority to work Incurs additional administrative overhead Risk of certificate revocation	[7], [10]
Manual Verification Schemes	***Manual Verification***	Analysis of user content	Low cost overheads	Possibility of new attacks Inappropriate for large-scale deployment/large datasets	-

TABLE III. SUMMARY OF SYBIL ATTACKS AND DEFENSE METHODS

Types of Sybil Attacks	**Defense Methods**
Routing	Graph-based detection methods
Distributed storage	Machine learning techniques
Data aggregation	Machine learning techniques
Voting/reputation systems	Graph-based techniques
Resource allocation	Prevention schemes and graph-based detection methods
Misbehavior detection	Graph-based detection and manual verification

4. Future Works

The overarching contribution of this paper is a survey of Sybil attacks in IoT and SMNs and potential solutions proposed to mitigate these threats. Therefore, the paper gives a general overview of the current state of knowledge in Sybil attacks. Future studies need to focus on the effectiveness of the defenses against a specific type of Sybil attack, both in IoT and MSN environments. The idea should be to evaluate the appropriateness of Sybil countermeasures against a particular kind of threat by comparing the features of existing defense systems. This should also encompass assessing the feasibility of combining two or more countermeasures to improve the effectiveness against targeted Sybil attack.

5. Conclusion

Sybil attacks present one of the most common security threats in IoT and MSNs. Currently, there is a lack of information on the best defense mechanisms against Sybil attacks. This research explores the current types of Sybil attacks, the potential defense mechanisms, and the proposed schemes. The findings indicate a broad range of Sybil attacks targeting various protocols and services, albeit using a common attack mechanism. The common Sybil attacks target routing, distribution storage, data aggregation, and resource allocation. The defense mechanisms fall into four broad categories: graph-based, Machine Learning, prevention, and manual verification methods.

References

[1] A. M., Bhise & S. D., Kamble. “Review on detection and mitigation of Sybil attack in the network.” In *International Conference on Information Security & Privacy (ICISP2015),* Nagpur, India, Procedia Computer Science, vol. 78, 2016, pp. 395-401.

[2] K. Zhang, X. Liang, R. Lu, & X. Shen. “Sybil attacks and their defenses in the Internet of Things”. *IEEE Internet of Things Journal,* vol. 1, no. 5, 2014, pp. 372-383.

[3] Y. Najaflou, B. Jedari, F. Xia, L. T., Yang, & M. S. Obaidat. “Safety challenges and solutions in Mobile Social Networks”. *IEEE Systems Journal,* 2013, pp. 1-13.

[4] K. Zhang, X. Liang, R. Lu, K. Yang, & X. Shen. “Exploiting Mobile Social Behaviors for Sybil detection”. In *the IEEE Conference on Computer Communications,* 2015, pp. 271-279.

[5] S. Trifunovic, & A. Hossmann-Picu. “Stalk me if you can – The anatomy of Sybil attacks in opportunistic networks”. In *Proceedings of the 9th ACM MobiCom Workshop on Challenged Networks,* 2014, pp. 37-42.

[6] W. Chang & J. Wu. “A survey of Sybil attacks in networks”. In *Sensor Networks for Development,* 2014, pp. 497-534.

[7] R. John, J. P., Cherian, & J. J. Kizhakkethottam. “ A survey of techniques to prevent Sybil attacks”. In *the IEEE International Conference on Computer Communications and Informatics,* Coimbatore, India, 2015.

[8] S. Sinha, A. Paul, & S. Pal. “The Sybil attack in mobile ad hoc network: Analysis and detection”. In 3rd *International Conference on Computational Intelligence and Information Technology, IET,* 2013, pp. 458-466.

[9] M. Al-Qurishi, M. AL-Rakhami, M. Alrubaian, & M. S., Hossain. “Sybil defense techniques in online social networks: A survey”. In *IEEE,* vol. 5, 2017, 1200-1027.

[10] S. Park, B. Aslam, D. Turgut, & C. C. Zou. “Defense against Sybil attack in vehicular ad hoc network based on roadside unit support”. In *IEEE Military Communications Conference (MILCOM), 2009,* pp. 1-7.

[11] A. Tangpong, G. Kasidis, & H. Hsun. “Robust Sybil detection for MANETs”. In *The Proceedings of the 18th International Conference on Computer Communications and Networks,* 2009, pp. 1-6.

[12] D. Quercia & S. Hailes. “Sybil attacks against mobile users: Friends and foes to the rescue”. In *IEEE INFOCOM Proceedings,* 2010.

[13] A. Chinchore, G. Xu, & F. Jiang. “Classifying Sybil in MSN using C4.5”. Thesis, University Technology of Sydney, 2016, June.

[14] S. Abbas, M. Merabti, D. L., Jones, & K. Kifayat. “Lightweight Sybil attack detection in MANETs. *IEEE Systems Journal,* vol. 7, no. 2, 2013, pp. 237-248.

[15] Y. Sun, L. Yin, & W. Liu. “Defending Sybil attacks in Mobile Social Networks.” In *IEEE Conference on Computer Communications Workshops,* 2014, pp. 163-164.

[16] A. Chinchore, F. Jiang, & G. Xu. “Intelligent Sybil attack detection on abnormal connectivity behavior in Mobile Social Networks.” *Springer International Publishing, Switzerland,* 2015, pp. 602-617.

[17] P. Gu, R. Khatoun, Y. Begriche, & A. Serhouchni. “Vehicle driving pattern based Sybil attack detection”. In *IEEE 18th International Conference on High Performance Computing and Communications,* 2016, pp. 1282-1288.

[18] P. Gu, R., Khatoun, Y., Begriche, & A., Serhrouchni. “Support Vector Machine (SVM) based Sybil attack detection in vehicular networks”. *Wireless Communications and Networking Conference* (WCNC), IEEE, 2017.

[19] Chinchore, A. A. Data Mining of Classification for Sybil User Detection. Thesis. University of Technology, Sydney, 2016, June.

[20] P. Gu, Khatoun, Y., Begriche, & A., Serhrouchni. “k-Nearest neighbor classification based Sybil attack detection in vehicular networks”. In *3rd International Conference on Mobile and Secure Services* (MobiSecServ), 2017.

[21] H. Yu, M. Kaminsky, P. B., Gibbons, & A. Flaxman. "SybilGuard: Defending against Sybil attacks via social networks". In *Proceedings of the 2006 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications,* 2006, pp. 267-278.

[22] H. Yu, P. B. Gibbons, M. Kaminisky, & F. Xiao. "SybilLimit: A near optimal social network defense against Sybil attacks". In *IEEE/ACM Transactions on Networking,* vol. 18, 2010.

[23] N. Z. Gong, M. Frank, & P. Mittal. “Sybilbelief: A semi-supervised learning approach for structure-based Sybil detection.” *IEEE Transactions on Information Forensics and Security,* vol. 9, 2014, pp. 976-987.

[24] B. Isaac & N. Israr. Case Studies in Secure Computing: Achievements and Trends. CRC Press, 2014.

[25] K. Xu. & H. Zhu. Wireless Algorithms, Systems, and Applications. Springer, 2015.

[26] J. Newsome, E. Shi, D. Song, & A. Perrig. “The Sybil attack in sensor networks: analysis & defenses”. In *IEEE International Symposium on Information Processing in Sensor Networks,* 2004, 6577-6580.