University of Sindh Journal of Information and Communication Technology
(USJICT)
Volume 5, Issue 2, July 2021

ISSN-E: 2523-1235, ISSN-P: 2521-5582
Website: http://sujo.usindh.edu.pk/index.php/USJICT/
© Published by University of Sindh, Jamshoro

An Insight into Sybil Attacks – A Bibliometric Assessment

Mahawish[1], Osama A Rehman[1], MuahmmadHassan Nasir [2]

[1]Department of Software Engineering, Bahria University, Karachi Campus, Sindh, Pakistan
[2]Department of Computer Science, NED UET, Karachi, Sindh, Pakistan
mahwishfatima.bukc@bahria.edu.pk,osamahussain.bukc@bahria.edu.pk,mhassan.cse@gmail.com

Abstract: Sybil attack poses a significant security concern in both centralized and distributed network environments. However, Sybil attacks poses a great impact on the privacy and trust of the network that results to lead confidentiality, integrity and authentication issues. In Sybil attack malicious adversary sabotage the network by impersonating itself as several nodes, called Sybil nodes. A sybil attacker creates different identities for a single physical device to deceive other benign nodes, as well as uses these fake identities to hide from the detection process, thereby introducing a lack of accountability in the network. In this paper, we have thoroughly discussed the sybil attack including its types, attack mechanisms, mitigation techniques that are in use today for the detection and prevention of such attacks. Subsequently, we have discussed the impact of the Sybil attack in various application domains and performed a bibliometric assessment in the top four scholarly databases. This will help the research community to quantitatively analyze the recent trends to determine the future research direction for the detection and prevention of such attacks.

Keywords: Security and privacy; Network security; Sybil Attack; Bibliometric Assessment;

I. Introduction

Many security solutions have been proposed to secure the network communication from various attacks[1]. The sybil attack has emerged as one of the most devastating attacks. In this type of attack, the attacker creates and controls multiple identities on the same device[2]. It occurs when there is a one-to-one correspondence between the entity and its identity is violated. Sybil attack was introduced by Douceur in 2002[3]. This type of attack is easy to launch (e.g., where sybil node makes illegal copies of identities to deceive the network) but difficult to detect. The consequence of Sybil attack degrades the network performance [4].

Sybil attacks affect various application domains and environments [5], for instance, the point-to-point (P2P) reputation system can be compromised as the attacker can favorably alter the reputation scores by the use of the newly created rogue identities [6].

In the modern era of smart devices, the security of unguided medium has become one of the prime concerns of network administrators due to the continuous deployment of wireless sensors and shared nature of the medium[7]. During passive monitoring, the malicious attacker gathers the identities network devices and further use them to launch Sybil attacks. With the recent advancement in technology, the distributed or pervasive computing provides many benefits such as data sharing, data availability and autonomy with increasing security risk which limits the use of distributed systems[8]. Sybil attack is one of the most prominent risks in these networks [3]. By initiating sybil attack, it is possible for an entity to unfairly present more than one identity. Similarly in Mobile Adhoc Network (MANET), because of lack of centralized authority, sybil nodes can mislead the honest nodes and resulting into node hijacking[9].

II. Contribution

In this study, we aim to present an in-depth understanding of the sybil attacks and its detection and prevention approaches with respect to their application domains to facilitate the research community to make the detection process more efficient and robust for state-of-the-art Sybil attacks. Accordingly, we make the following major contributions in this study:

- Presenting an insight into the Sybil attack types, mechanisms and mitigation strategies as well as its impact in four major domains including Internet of Things (IoT), Wireless Sensor Networks (WSN), Blockchain and Intelligent Transportation System (ITS).
- A review with sufficient depth and breadth of the existing state-of-the-art approaches found in the literature concerning detection or prevention of such attacks with respect to various application domains.
- dispense of research trends through bibliometric assessment of the articles published between 2014 to 2020 in four major scientific digital libraries including IEEE, Springer, ACM and Elsevier.

To this end, we summarize the organization of the rest of this paper. In Section III we review existing work done for the detection and prevention of Sybil attack, In Section IV we discuss the sybil attacks, including its types, attack mechanism and mitigation techniques. In section V we discuss sybil attack effects on different application domains. Section VI contains trend assessment in four popular digital libraries including Elsevier, IEEE, Springer and ACM. The last section contains general conclusions and future work.

III. RELATED WORK

This section elucidates some of the existing state-of-the-art approaches employed for detection and prevention of sybil attacks within different application domains as shown in table 1.

Such as in paper [6], the author proposed distributed detection scheme for both static and mobile nodes where in first step each node collect Received Signal Strength Indicator (RSSI) information and in second step share this information with its nearby neighbor. For message authentication either symmetric or asymmetric encryption technique is used. In the last step RSSI ratio is calculate among nodes using shared information that decides whether a node is benign or attack.

In paper [25], the proposed method uses symmetric key cryptography algorithm to prevent sybil attack in the network, a key is given to each individual node before a node start communicating over network. A key is only given to authentic node after a successful verification of its identity.

In paper [4], the proposed technique prevents an attacker to join the group of the legitimate user on social networks by implementing pair based cryptography authentication process, where each legitimate user gives feedback for a new user who wants to join network. The proposed technique guards the social network from sybil attack and prevents forge identities.

In paper [29], author proposed a community based sybil detection in the network. It divides the network into communities and use persuading function to determine the attack edge. Community detection algorithm results in fast detection of communities within the network with low computational complexity.

1. To identify potential attack edge: Firstly, Compute the persuading function for all nodes (represented as x) in all community denoted as k.
2. If fx,k(N, nk) > γ (a predefined threshold) then all edges from community k to node X will be labeled as potential attack.
3. Community with more potential attack edges is labeled as Sybil community. In [24], author proposed enhanced Ad-hoc On-demand Distance Vector (AODV) protocol which is based upon the behavioral profiling of an attacker. Network parameters are used to identify attacker behavior. Trust based approach has been used in order to differentiate attacker and legitimate user. A node with low trust value will be discarded and packets will be rerouted through trust based nodes. Each node has vector consists of hop-count and trust value. Three types of trust are there:

- Directed trust
- In-directed trust
- Recommended trust

The route selection conditions are:

- No. of Hop count for Nodes are same, Node with highest trust will be selected.
- Nodes with same trust value but different hop count. Minimum hop count value node will be selected.
- Nodes with different hop count and different trust value (based upon trust approach). In paper [15], author proposed a sybil attack prevention mechanism for dynamic network specially Vehicular Adhoc Network (VANET). The working mechanism of proposed method is validating the Media Access Control (MAC) ID of a vehicle For example if a vehicle or node request Road Side Unit (RSU) to join the network, the RSU ensures for the validity of vehicle's MAC address. If it validates then an encrypted message with ID is sent to vehicles' On-Board Units (OBU), the OBU send it to RSU for further verification. After the completion of the verification phase, a vehicle can send data on the network.

In [1], trust based scheme has been used to identify Sybil and rank attack which is very common in Routing Protocol for Low-Power and Lossy Networks (RPL). The technique works on direct, indirect and recommended trust. Author implemented a test-bed approach in his paper.

In [37], author proposed a self-learning Intrusion Detection System (IDS) to detect sybil node in vehicular ad-hoc network [39]. Proposed IDS consists of Long Short Term Memory (LSTM) neural network where relevant information from large number of Cooperative Awareness Message (CAM) extracted including car trust value, ID, location, driving position, speed and etc. This information is collected and used for training a LSTM neural network based IDS, the trained IDS is capable enough to take decision either a car is black-listed or white-listed.

In [23], author proposed an IDS named SHA-EIoT to protect the IoT environment from sinkhole attack. Proposed methodology consists of two phases; in first phase algorithm-1 identifies the presence of suspicious nodes by using various parameters, such as node identity, hop count from remaining energy at nodes and rank information to identify the presence of sink hole attacker. In second phase algorithm- 2 confirms the presence of attacker, If an edge node does not receive data packets from a suspicious node, it indicates that suspicious node is sinkhole attacker because it consumes all packets and does not forward packets towards the destination.

Table 1 Existing work related to Sybil attack

Paper	Mechanism	Technique	Attack type	Application domain	Tool	Accuracy	Year
[6]	Detection	Cryptography	Sybil detection for direct & indirect Sybil identities	IoV and IoT	-	100%	2006
[25]	Prevention	Cryptography	Sybil attack	Wireless Sensor Network	-	-	2015
[4]	Prevention	Cryptography	Sybil attack	Online Social Network	-	-	2015
[29]	Detection	Persuading Function	Sybilcommunity detection	IoT system	Monte carlo simulation	70%	2016
[24]	Detection	Trust based technique	Sybil attack	Smart Heath care IoT	NS2	99.7%	2017
[15]	Prevention	Cryptography	Sybil attack	VANET	-	-	2018
[1]	Detection	Trust based technique	Rank & Sybil attack detection	MANET, WSN	Contiki &Cooja	73%	2019
[37]	Detection	Trust based technique	Sybil attack	VANET	NS2 & SUMO	95%	2020
[23]	Detection	Network Traffic parameters	Sybil attack, sinkhole	Surveillance, security & monitoring systems	NS2	95.83%	2020

IV. SYBIL ATTACK

In sybil attack, a sybil node makes illegal copies of identities to deceive the network. Sybil attack is one of the most prominent risks in these networks [7]. By initiating sybil attack, it is possible for an entity to unfairly present more than one identity, as shown in figure 1, node C and node D are malicious nodes have many fake identities

e.g. C = C1, C2, and D = D1, D2, D3 to deceive voting system in order to get the desired result by casting fake votes. Although Sybil attack are diverse in nature but they involve almost similar strategies to launch an attack. The aim of attacker is to create multiple fake copies by forging the identities of other systems as shown in figure 1, first of all they create link to the normal or honest nodes. Next, they create fake identities, these fake identities look like the identity of normal nodes, once the identity is compromise the normal node turn to sybil node. On the other hand attacker node uses its real identity to communicate in the network and malicious attacker uses sybil identities to deceive other nodes in the network.

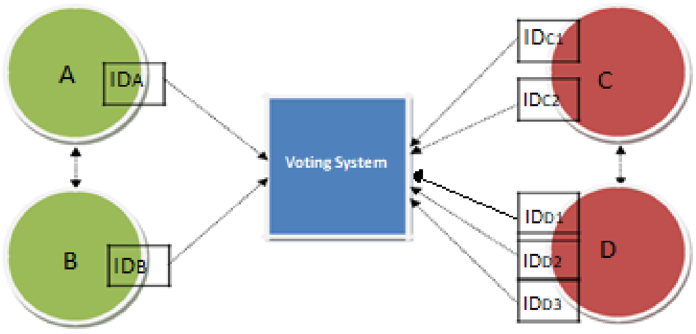

Figure 1 Sybil nodes in Voting System

A. *Types of Sybil Attack*

In sybil attack, the attacker or malicious network node impersonate other nodes and the node whose identity is being spoofed is known as sybil node [8]. There are different ways by which a sybil attack can be initiated; the section presents a comparative-taxonomy of various types of sybil attacks.

1. *Insider Attack vs. Outsider Attack*

In an insider attack as shown in figure 2, the sybil attacker holds one valid identity with a claim that it receives data via various counterfeit identities. Since in a distributed system every network node is considered trustworthy allowing false data to be propagated to the network. In case of an outsider attack, the attacker must gain access to them by understanding all the security mechanism such as authentication policy of the network before launching an attack [5].

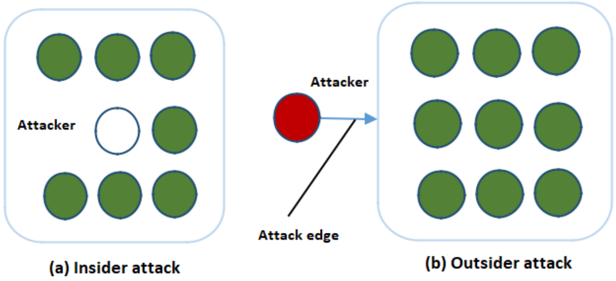

Figure 2 Insider vs. Outsider attack

2. *Directed vs. In-directed Communication*

The communication strategy of sybil nodes with legitimate nodes are of great importance in devising countermeasures of sybil attacks. The communication can be directed or in-directed, as shown in figure 3, means the attacker can communicate with a legitimate node directly via fake sybil identities, or use real identity to send sybil data with other legitimate nodes [32].

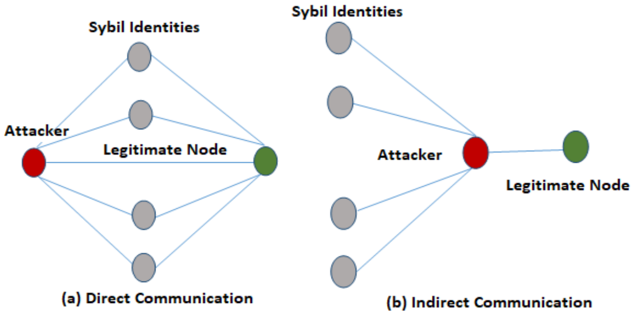

Figure 3 Direct vs. Indirect communication

3. *Simultaneously vs. Gradually Obtained Sybil Identities*

There are two ways to generate sybil identities, either all at once or gradually as shown in figure 4. The sybil nodes are more difficult to detect if the node has more diverse feature set. The gradual creation of sybil nodes may increase the attack time as well as explosion time of some sybil nodes. The chance of sybil identities being identified is high if a mechanism of random verification of the authenticity of nodes identities is in place [35].

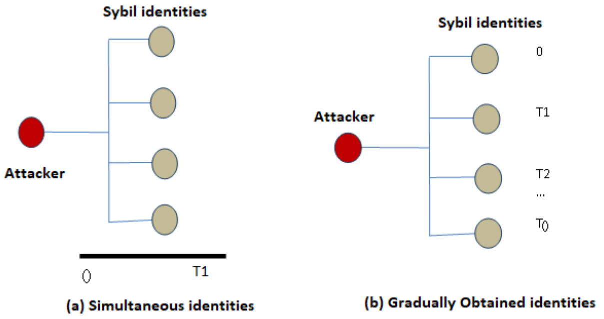

Figure 4 Simultaneous vs. Gradually obtained identities

4. *Busy vs. Idle*

The choice of using all sybil identities or some of them to launch an attack depends upon how easy is to obtain an identity as shown in figure 5. If an attacker creates lots of sybil identities then idle sybil node could help them to look more real. Since the strength of the attack relies upon the number of identities. On the other hand, if the attacker does not have sybil identities in large quantities then he has to use all of them to launch an effective attack [13].

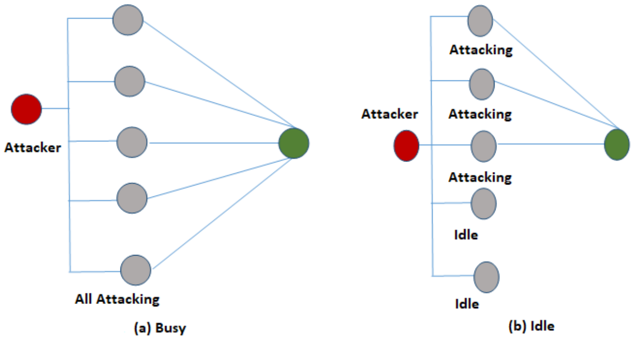

Figure 5 Busy vs. Idle

B. *Attack Mechanisms*

Following are the attack mechanism in Sybil attack.

1. *Distributed Storage*

In this mechanism, a system that is designed to replicate or fragment data in several nodes are affected by a malicious attacker, who can easily defeat replications and fragmentation process and can store all data on his node and temper it according to his desire [16].

2. *Routing*

Sybil attack is used against routing mechanism e.g., multipath and geographic routing is most vulnerable, where instead of having one set of coordinates, Sybil node appears at multiple locations at one time. In this way, the malicious node isolates one part of the network by sending malicious replay [10].

3. *Data Aggregation*

In this mechanism, using a sybil attack, an attacker node can contribute many times to compute and aggregates the sensor readings and can alter these reading by using his sybil identities [2].

4. *Resource Allocation*

This attack mechanism is used to obtain an unfair share of network resources such as sharing of the single radio channel, where every node is permitted to transmit data as per given time slot. But due to the presences of sybil attacker the network resources are not shared among legitimate nodes and their share obtrusively taken by an attacker [19].

C. *Mitigation Techniques*

Since the arrival of the sybil attack, various methodologies are being developed to identify, detect and prevent this type of attack [34]. Some of the mitigation approaches are given in figure 6.

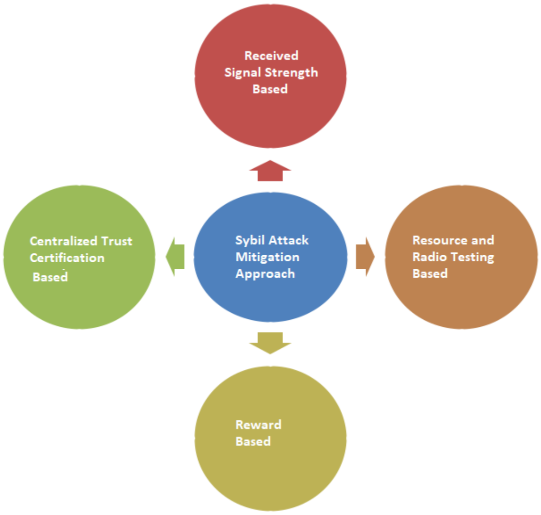
Received Signal Strength Based
Centralized Trust Certification Based
Sybil Attack Mitigation Approach
Resource and Radio Testing Based
Reward Based

Figure 6 Mitigation techniques

1. Centralized Trust Certification Based Approach

Douceur [7] proposed a solution which uses a central authoritative entity to authorize other nodes in the network. Authentication is based on asymmetric key cryptography. Each node in the network has been assigned an exclusive digital signature. However, this approach is not efficient in terms of cost when implemented to the large-scale networks.

2. Received Signal Strength-Based Approach

A robust, light-weight methodology with increased accuracy based on the received signal strength of communication messages to cope with sybil attack issue is proposed by Demirbas et al [6]. The collaboration among messages and the additional node is making this scheme successful but on the other hand, generates false-positives, which makes the scheme unreliable.

3. Resource and Radio testing Based Approach

Newsome [19] suggested a resource testing mechanism as a countermeasure of sybil attack which consists of two schemes: first consists of a verification node to evaluate resources (storage, energy, capacity, etc.). A node is considered as an attacker if it has higher resources than starved nodes are found but these verification messages may congest the network [38]. This can be prevented by setting every node with only one radio channel from which it can transmit or receive.

4. Reward-based Approach

Reward-based or the incentive-based approach is based on economic reward. The protocol offers an incentive to the attacker node on the revealing of identities controlled by him. The target peer name is affirmed when incentive or reward received by the attacker [31].

V. GENERAL IMPACT OF SYBIL ATTACK IN VARIOUS APPLICATION DOMAIN

Sybil attacks has significant impact on various application domain e,g., Internet of Things (IoT), Wireless Sensor Network (WSN), Blockchain, and Intelligent Transportation System (ITS). Discussion related to aforementioned domains is given below.

A. Internet of Things

IoT has a great impact in today’s modern world, it not only has changed the living style of individuals but also changed the way we do business. Millions of smart devices, sensors, actuators, etc. are manufactured every year that assists humans to smoothly perform business activities, control and monitor home appliances, grids, and human health. However, with the great advantages, there is an intrinsic security threat due to the resource-constrained nature of IoT devices that limits the available security solutions implemented in IoT based systems [24].

B. WSN

WSNs have developed significantly in re-cent years and have significant potential in a variety of applications, including health, the environment and the military. WSN performs powerful functions that include network monitoring, network state information collection, data transmission, object tracking, and positioning, so security is a challenging task that cannot be ignored [29] In order to strengthen the security mechanism, it has been suggested in the past that all nodes be cooperative and trust- worthy. Many attacks can take place in WSN but the most common attack is sybil attack. Sybil attack in WSN can create false identity nodes or by stealing the legal identities of other nodes. Some of the solutions for the detection of WSN attacks are distance vector hop which can detect and provide defense sybil attack [22]. The other detection mechanism being used in recent years is Received Signal Strength Indicator (RSSI) which is considered as the light-weight process for the detection of sybil attack [21].

C. Blockchain

The blockchain is a distributed ledger technology which is emerging as a disruptive approach that offers features including decentralization, immutability, and temper resistant database. The blockchain was first devised for crypto-currency named Bitcoin by a scientist psudo-named Sakoshi Nakamoto in 2008 [18]. However, this technology has evolved and now being successfully adopted in various non-crypto-currency domains due to its intrinsic feature set. The technology consists of chain of blocks that contains a number of transactions and a link to previous block. The block/transactions can only be added or deleted to the chain after validation process, called consensus, by all mining nodes within the network. This type of structure adds enormous amount of security, audit and pre-vents data to be altered. However, the blockchain based systems are still prone to sybil attacks, where malicious adversaries use fake identities to influence the decision of entire blockchain network [26]. There are various available solutions but they have their pros and cons, for instance, one of the recent work to for mitigation of sybil attacks is by Otte et al. [20] which prevents these attacks by adding trust . However, the chain performance decreases upon increase in ledger size. Therefore an effective sybil resistant mechanism is deemed essential for blockchain to reach its true disruptive potential.

D. ITS

ITS is a network of connected vehicles. In this network vehicles can communicate among one another. The main services of ITS include traffic information services, partially autonomous vehicles support, improvement in road-safety, and improved traffic management system. The communication paradigm of these applications includes sensors for real-world conditions which is then communicated on a ubiquitous network. The network then marks each vehicle with a separate wireless interface, which creates a dynamic ad-hoc network which is then referred to as VANET [9]. These are a special type of MANET that can communicate between neighboring vehicles and roadside equipment. Sybil attack is one of the most dangerous attacks in VANET. In a sybil attack, the attacker can shape the network as per their needs [34]. There are many ways for detecting malicious vehicles in VANET in which some of the proposed methodologies in recent years are sybil node detection based upon Driving Pattern Matrices (DPMs) [11], using machine learning [33], etc.

VI. Survey Results

The bibliometric assessment is a popular way to make progression and analyze the past researches in a particular area by examining the relationship amongst various variables such as fields, individual papers, journal, annual scientific productions and etc.

In this paper, we have selected top four scientific libraries including IEEE, Springer, ACM and Elsevier to find out the annual scientific paper production for sybil attack. Based on the following search queries:

- ***(”Sybil attack” AND (”IoT” OR ”Internet of Things”) NOT ”Blockchain” NOT ” Wireless Sensor Network” NOT ”Intelligent Transportation System”)***
- ***(”Sybil attack” AND ”Blockchain” NOT (”IoT” OR ”Internet of Things”) NOT ” Wireless Sensor Network” NOT ”Intelligent Transportation System”)***
- ***(”Sybil attack” AND ” Wireless Sensor Network” NOT (”IoT” OR ”Internet of Things”) NOT ”Blockchain” NOT ”Intelligent Transportation System”)***
- ***(”Sybil attack” AND ”Intelligent Transportation System” NOT (”IoT” OR ”Internet of Things”) NOT ”Blockchain” NOT ” Wireless Sensor Network”).***

The annual scientific production provides a broad way to devise conclusions based on analyzing the publication trends by observing year-wise publication of articles from digital libraries in the desired domain. We searched four scientific databases (mentioned in previous section) to identify the number of articles published from 2014 to 2020.

The total articles in each databases is illustrated in figure 7. The Springer and Elsevier yields most results which is 563 and 559 respectively in the selected criteria. The IEEE Xplorer and ACM yield 320 and 209 articles.

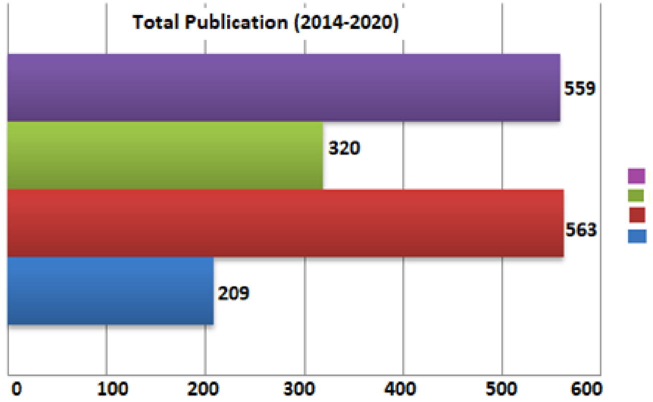

Figure 7 Total publications

The figure 8 shows a comparison of publication trends in terms of publications per year. The comparison result shows the exponential growth in the published articles from 2014 to 2020 in all 4 libraries. Moreover, the graph also shows that the global publication touched its peak during the year 2019.

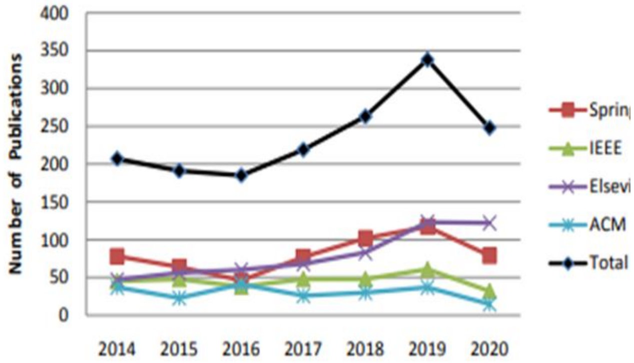

Figure 8 Comparison of research trends in Sybil Attacks

Through our research, we also have identified four major domains, as shown in figure 9, including IoT, Blockchain, WSN and ITS in which the research articles are published. The WSN is the domain, consists of 47% of the research share, in which the most articles are published. The IoT, which is considered as a sub-domain of WSN, consists of 24% articles. The blockchain is another area, consists of 22% articles, which is prone to Sybil at-tacks. The ITS consists of 7% of articles. The trend shows that the WSN and IoT are the most vulnerable domains consists of a total 71% articles and the researchers are focused to find out the ways to mitigate such kind of attacks.

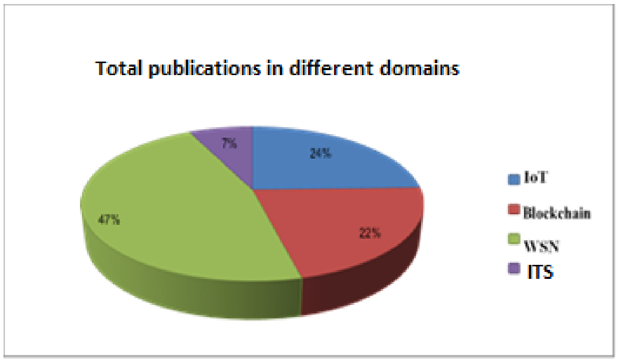

Figure 9 Total publications w.r.t different domains

VII. CONCLUSION AND FUTURE DIRECTION

In recent years, the Sybil attacks have become one of the prime concerns for ensuring network security. This paper has contributed by identifying the attack vectors in terms of highlighting the Sybil attack types along with some of the known attack mechanisms. Different tools and techniques is also presented in table 1. Survey of various detection and prevention techniques showed that trust based approach for Sybil attack detection and cryptography approach for prevention are widely used techniques. The paper also presented a brief bibliometric assessment that highlights the publication trends within four most popular digital libraries including IEEE, Elsevier, ACM, and Springer which shows the exponential growth in the publications per year. The research also showed that the global publication touched its peak during the year 2019. Through our study, we have elucidated four major domains including Blockchain, WSN, IoT, and ITS that are the most vulnerable attack surfaces and require further attention from the research community to devise an effective mechanism so as to prevent such kind of attacks. Moreover, we have found that recent trends of attack show that sybil attack had great raise in 2019. Our future work involves an in- depth comparative study consists of SWOT analysis of various mitigation mechanisms within IoT that helps the research community to devise an effective Sybil attack avoidance, prevention, and detection mechanism to timely and efficiently mitigate such attacks.

REFERENCES

[1] Airehrour D., Gutierrez J.A., Ray S.K.: SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. In: Future Generation Computer Systems, vol. 93, pp. 860–876, 2019.

[2] Al-Hamadi H.H.: Dynamic Redundancy Management of Multisource Multipath works. Ph.D. thesis, Virginia Tech, 2014. Routing Integrated with Voting-based Intrusion Detection in Wireless Sensor Network.

[3] Al Shehri W.: A survey on security in wireless sensor networks. In: International Journal of Network Security & Its Applications (IJNSA), vol. 9(1), pp. 25–32, 2017.

[4] Alrubaian M., AL-Qurishi M., Md S., Rahman S.M.M., Alamri A.: A Novel Prevention Mechanism for Sybil Attack in Online Social Network. 2015.

[5] Chang W., Wu J.: A survey of sybil attacks in networks, 2014.

[6] Demirbas M., Youngwhan Song: An RSSI-based scheme for sybil attack detection in wireless sensor networks. In: 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks(WoWMoM'06), pp. 5 pp.–570. 2006.

[7] Douceur J.J.: The Sybil Attack. In: , 2002. URL https://www.microsoft.com/ en-us/research/publication/the-sybil-attack/.

[8] Faisal M., Abbas S., Rahman H.U.: Identity attack detection system for 802.11- based ad hoc networks. In: EURASIP Journal on Wireless Communications and Networking, vol. 2018(1), p. 128, 2018.

[9] Feng X., Li C.y., Chen D.x., Tang J.: A method for defensing against multi- source Sybil attacks in VANET. In: Peer-to-Peer Networking and Applications, vol. 10(2), pp. 305–314, 2017.

[10] Ferng H.W., Rachmarini D.: A secure routing protocol for wireless sensor net- works with consideration of energy efficiency. In: 2012 IEEE Network Operations and Management Symposium, pp. 105–112. IEEE, 2012.

[11] Gu P., Khatoun R., Begriche Y., Serhrouchni A.: Support vector machine (svm) based sybil attack detection in vehicular networks. In: 2017 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–6. IEEE, 2017.

[12] Isaac J.T., Zeadally S., Camara J.S.: Security attacks and solutions for vehicular ad hoc networks. In: IET Communications, vol. 4(7), pp. 894–903, 2010.

[13] Jhaveri H., Jhaveri H., Sanghavi D.: Sybil attack and its proposed solution. In: International Journal of Computer Applications, vol. 105(3), 2014.

[14] John R., Cherian J.P., Kizhakkethottam J.J.: A survey of techniques to prevent sybil attacks. In: 2015 International Conference on Soft-Computing and Networks Security (ICSNS), pp. 1–6. IEEE, 2015.

[15] Khalil M., Azer M.A.: Sybil attack prevention through identity symmetric scheme in vehicular ad-hoc networks. In: 2018 Wireless Days (WD), pp. 184–186. IEEE, 2018.

[16] Khan S., Gani A., Wahab A.W.A., Shiraz M., Ahmad I.: Network forensics: Review, taxonomy, and open challenges. In: Journal of Network and Computer Applications, vol. 66, pp. 214–235, 2016.

[17] Krombholz K., Hobel H., Huber M., Weippl E.: Advanced social engineering attacks. In: Journal of Information Security and applications, vol. 22, pp. 113–122, 2015.

[18] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." *Decentralized Business Review* (2008): 21260.

[19] Newsome J., Shi E., Song D., Perrig A.: The Sybil Attack in Sensor Networks: Analysis Defenses. In: Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, IPSN 04, p. 259268. Association for Computing Machinery, New York, NY, USA, 2004. ISBN 1581138466.

[20] Otte P., de Vos M., Pouwelse J.: TrustChain: A Sybil-resistant scalable blockchain. In: Future Generation Computer Systems, vol. 107, pp. 770–780,2020.

[21] Patel A., Taghavi M., Bakhtiyari K., Ju´Nior J.C.: An intrusion detection and prevention system in cloud computing: A systematic review. In: Journal of network and computer applications, vol. 36(1), pp. 25–41, 2013.

[22] Patel S.T., Mistry N.H.: A review: Sybil attack detection techniques in WSN. In:(ICECS), pp. 184–188,

2017. 2017 4th International Conference on Electronics and Communication Systems.

[23] Pundir S., Wazid M., Singh D.P., Das A.K., Rodrigues J.J., Park Y.: Designing Efficient Sinkhole Attack Detection Mechanism in Edge-Based IoT Deployment. In: Sensors, vol. 20(5), p. 1300, 2020.

[24] Rajan A., Jithish J., Sankaran S.: Sybil attack in IOT: Modelling and defenses. In: 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 2323–2327. 2017.

[25] Rathee P., Malhotra S.: Preventing sybil attack in wireless sensor networks. In: International Journal for Innovative Research in Science & Technology, vol. 1(12), 2015.

[26] Salah K., Rehman M.H.U., Nizamuddin N., Al-Fuqaha A.: Blockchain for AI: Review and open research challenges. In: IEEE Access, vol. 7, pp. 10127–10149, 2019.

[27] O. Sbai and M. Elboukhari, "Classification of Mobile Ad Hoc Networks Attacks," *2018 IEEE 5th International Congress on Information Science and Technology (CiSt)*, 2018, pp. 618-624,

[28] Sharma P.K., Moon S.Y., Park J.H.: Block-VN: A distributed Blockchain based vehicular network architecture in smart city. In: Journal of information process- ing systems, vol. 13(1), 2017.

[29] Silawan T., Aswakul C.: Sybilcomm: Sybil community detection using persuad- ing function in iot system. In: 2016 International Conference on Electronics, Information, and Communications (ICEIC), pp. 1–4. IEEE, 2016.

[30] Tangpong, Athichart. "Managing sybil identities in distributed networks." (2009).

[31] Toyoda, Kentaroh, and Allan N. Zhang. "Mechanism design for an incentive-aware blockchain-enabled federated learning platform." *2019 IEEE International Conference on Big Data (Big Data)*. IEEE, 2019.

[32] Trifunovic S., Hossmann-Picu A.: Stalk and lieThe cost of Sybil attacks in op- portunistic networks. In: Computer Communications, vol. 73, pp. 66–79, 2016.

[33] Yang Z., Zhang K., Lei L., Zheng K.: A novel classifier exploiting mobility be- haviors for Sybil detection in connected vehicle systems. In: IEEE Internet of Things Journal, vol. 6(2), pp. 2626–2636, 2018.

[34] Yao Y., Xiao B., Wu G., Liu X., Yu Z., Zhang K., Zhou X.: Multi-channel based Sybil attack detection in vehicular ad hoc networks using RSSI. In: IEEE Transactions on Mobile Computing, vol. 18(2), pp. 362–375, 2018.

[35] Zhang J., Zhang R., Sun J., Zhang Y., Zhang C.: Truetop: A sybil-resilient system for user influence measurement on twitter. In: IEEE/ACM Transactions on Networking, vol. 24(5), pp. 2834–2846, 2015.2

[36] Zhang K., Liang X., Lu R., Shen X.: Sybil Attacks and Their Defenses in the Internet of Things. In: IEEE Internet of Things Journal, vol. 1(5), pp. 372–383, 2014.

[37] Zhang Y.Y., Shang J., Chen X., Liang K.: A Self-Learning Detection Method of Sybil Attack Based on LSTM for Electric Vehicles. In: Energies, vol. 13(6), p. 1382, 2020.

[38] Mala, I, et al. "Fuzzy Logic Based Obstacle Avoidance Autonomous Robots." *Sindh University Research Journal-SURJ (Science Series)* 51.01 (2019)

[39] H. Nasir, Mahawish, S. S. Zia, M. Naseem, I. Mala "Intrusion Detection: Tools, Techniques and Trends" *Sindh University Research Journal-SURJ (Science Series)* 51.01 (2019)