A REVIEW ON THE DETECTION AND PREVENTION TECHNIQUE OF SYBIL ATTACK

Paramveer Singh Deswal[1], Bindu Rani[2], Manish Rai[3]

[1] Deptt. of CSE, BERI, Bhabha University, Bhopal

[2]Assistant Professor, Deptt. of CSE,GJUS&T,Hisar

[2]Assistant Professor, Deptt. of CSE, BERI, Bhabha University, Bhopal

Abstract

As the world is getting more and more digital day by day, the security of the information becomes the priority for the service providers. There can be attacks on the network in many forms to steal the information. One such attack in which a functioning node's identity is impersonated or hacked by the attacker to provide the trustworthy transmission of the information is called Sybil attack. There are many techniques and algorithms to detect and prevent the Sybil attack. But every technique or algorithm so far used has been ineffective to stop the Sybil attack completely. This paper has been written after studying and analyzing various techniques proposed for the detection and prevention of Sybil attack in various networks i.e., Wireless Sensor Network (WSN), Online Social Network (OSN), Mobile Ad hoc Network (MANET).

Keywords: *Sybil attack, wireless sensor network, suspicious node, online social network, Mobile Adhoc Network.*

1. Introduction

The data transmission field has become so vast that the security of the data has become more priority than sending it. There are many types of networks in which data can be transmitted. Some of the networks that are studied and discussed are Wireless Sensor Network (WSN), Online Social Network (OSN), Mobile Ad Hoc Network (MANET). All these networks are prone to data theft by some attacks. These attacks can be Denial-of-service, Jamming the signal to damage the network, Sybil attack where the attacker possesses the identity of a legitimate node and try to steal the data pretending to be the legitimate node, blackhole attack in which the attacker traps all the data and stop the transmission to the further nodes, Wormhole attack in which the attacker creates a tunnel which is shorter than the actual route which disturbs the routing mechanism that depends on the information about the various node distances. This corrupts the entire network[1][2].

Some of the networks studied in this paper are discussed below:

1.1. Wireless Sensor Network: Wireless sensor network is the collection of numerous micro sensing nodes which have the capability to sense, process data and communicate with other sensing nodes. These sensing nodes are also used in monitoring the physical and surrounding factors like temp., pressure, motion, etc. This information is cooperatively pass to a main location called a base station or sink. This base station is used to analyse the data passed by sensor nodes and the useful information is sent to the user whenever a query is made by the user. Radio signals are used by sensor nodes to communicate with

each other. A single wireless sensor node contains sensing and computing devices, radio transceiver, and power components. The individual node in wireless sensor networks is resource-constrained: limited processing speed, storage capacity, communication bandwidth. Once these nodes are deployed, it is their responsibility to self-organize a suitable network structure often with multi-hop communication with them. In Figure 1 shows how sybil attack occurs in wireless senor network is given below[3].

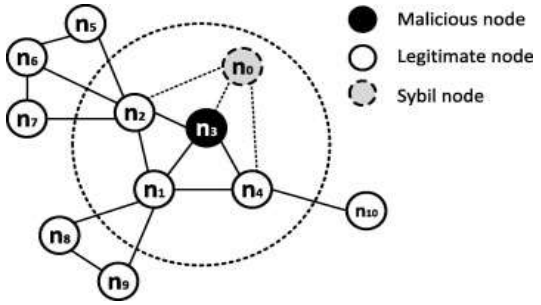

Figure 1: Sybil Attack in Wireless Sensor Network.

1.2. Mobile Ad hoc Network: Mobile Adhoc Network (MANET) has a routable networking environment on top of a link-layer Adhoc network. A set of mobile nodes is connected wirelessly in a self-healing and self-configured network without any fixed infrastructure. All MANET nodes can move freely due to the frequent change in the network topology. The connection is made in open-air through radio signals show it becomes easy for the taker to steal the information. Sybil attack is one such attack that causes much destruction to the connection. Sybil attack uses multiple identities at a single time and creates lots of disturbance among other notes or it sometimes acquires the identity of a legitimate node and gives a false expression of that node in the network. Figure 2 given below describes how sybil attack occur in Mobile Adhoc Network[4].

Figure 2: Sybil Attack in Mobile Adhoc Network.

1.3. Online Social Network: It is a kind of network in which people are connected in real life for making connections. People are directly connected through some online networks like Facebook, Instagram. Accounts are created to connect with other people. Each account is called a node and the connection is done through links. This type of network is more prone to attacks as it becomes difficult to recognize the credibility of a node. An attacker can create a fake account and send a request to a verified user. Many miscreants sell the legitimate note accounts online to the attacker. This could increase the attack capacity. Figure 3 given below describes how sybil attack occurs in Online Social Network[5].

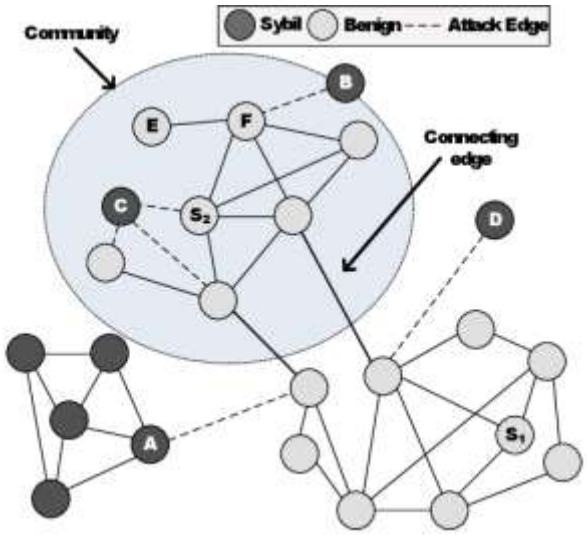

Figure 3: Sybil Attack in Online Social Network.

2. Sybil Attacks and its Types

Sybil attack is defined as the suspicious node which illegally takes multiple identities of legitimate node and steals the information or corrupts the network. This attack is done in three types which are listed below:

2.1. Direct and Indirect Attack: In Direct attack, the legal node communicates directly to the malicious node. In an indirect attack, the malicious node acts between the communications.

2.2. Fabricated and Stolen Identity Attack: New illegal nodes are created using the legal identities of the original node. For example, if an original node has an ID of 32-bit integer then it creates the exact ID of a 32-bit integer, it is known as fabricated nodes. In stolen identity, the attacker impersonates the legal node and then acts as a malicious node. The attack can remain undetected if the node is destroyed whose credential has been stolen.

2.3. Simultaneous and Non Simultaneous Attack: In simultaneous, the participation of all malicious nodes occur at same time in the network. While in Non-simultaneous attack, few malicious nodes take participation in the attack.

3. A Literature Review for detection and prevention of Sybil attack

Many researchers over the time as studied and developed several techniques to detect and prevent the occurrence of Sybil attack in the network. These techniques have many advantages over previous techniques and few disadvantages which led to further study in the field. The related work of several researchers has been studied with much grief and listed below.

1. Amuthavalli et al. [6] proposed RPC in which the location of nodes is controlled and deployed by RPC. Each node ID, the time, and a password is stored in a routing table that is generated by the RPC algorithm. All the in-between nodes from sending and receiving positions are identified. Then the RPC database compares the information of the intermediate node. If there is a match then the node is

labelled as a normal node otherwise it is said to be a Sybil node. After every small interval of time, a new password for each node is generated by the Random Password Generator and is sent to every node in the network. While the destination node is communicating with the source node, the destination node ID, time delay, and the random password corresponding to time-delay are compared with the RPC database. If there is a match of information, the sender will transmit else the receiver is marked as Sybil node.

2. Manju VC et al. [7] proposed CAM (Compare and Match Approach) and PVM (Position Verification Method) to detect and prevent these attacks. In CAM, all nodes are connected through edges. All the nodes have dynamic Key values given by the Base station. Whenever a node communicates with other nodes. This dynamic key value is given for communication. If the given key-value does not match with the key-value given by the Base station. It is considered as a Sybil node. The author also uses PVM, in this method, a node provides its original location whenever it wants to communicate with other nodes. This is because a Sybil node always possesses multiple identities.
3. Udaya Suriya raj Kumar Dhamodharan et al. [8] proposed CAM and PVM technology with Message Authentication and Passing (MAP) for detecting, eliminating, and eventually preventing the entry of Sybil attack in the network. In a network, source node 'A' passes data to destination node 'B'. The source node A sends a request message to destination node B with its key as msg(A) which is generated by the Base station while registering in the network. The destination node B submits its key message with msg(B) and later both keys are verified by the Base station and an OK signal is produced for sharing the data and any other information. Data transmission occurs between A and B once they get the signal from the base station.
4. Roopali et al. [9] proposed a lightweight technique by adding two more parameters that are energy and frequency. In this, when a node enters a network, its speed, energy, and frequency are checked. If the value of all three is greater than or equal to the threshold value then the node is considered as simple node otherwise as legitimate now.
5. Anamika et al. proposed a technique in which the detection of a Sybil node can be done from any node. The sender node verifies each node before sending the information to the receiver. Firstly it broadcast a request packet asking for a reply message which has a logical address (IP) and physical address (MAC) of all nodes. A table is maintained of the replies by the sending node. If any node with same physical address (MAC) reply with different logical address (IP) then the node with different logical identity is considered as Sybil node and sender node select an alternate path for transmitting packets to the destination.
6. Moshin et al. [10] proposed a Reduced Signal Strength (RSS) technique to differentiate between legal nodes and sybil nodes using a network simulator. The accuracy count is distributed by sybil attack by enhancing its trust and reducing others or capturing the identity of a few mobile nodes in MANET. It results in big information loss causing a delusion in the network. It also reduces the reliability of mobile nodes. RSS use three network condition like standard network behaviour, existence of malicious nodes in the network, and reduced signal strength. RSS works efficiently and does not have any data loss.
7. Dhanalakshmi et al. [11] proposed the RAI Tactic and LV Technique to prevent Sybil attack. In Relate and Identity Tactic, each system is provided a dynamic primary value by the base station. When the systems start communicating with each other, every system gives its primary value. If the primary value does not match with the primary value given by the base station, the system is considered as Exploited system. In Location Verification Technique, the location of nodes is used to

identify the Sybil system. Few times, the Sybil node is not detected by RAI, the LVT is used to carry out further detection.

8. Zhi Yang et al. used a vote trust algorithm to detect the Sybil attack. Vote trust is done using Vote capacity and Global Acceptance Rate (GAR). The Vote propagation is done to other neighbouring nodes from trusted seeds. If Global Acceptance Rate (GAR) is less than the threshold. It is considered a Sybil node. Now, this vote trust is used to detect the whole Sybil community. In the Friend Invitation Graph once some Sybil nodes are identified using vote trust detection. Vote Trust employs two key techniques, Bad Score Propagation and Sybil community identification, to correctly expand the Sybil community and to determine its boundary.
9. Anagha P B et al. [12] proposed the Vote Credence technique in which the vote trust algorithm is further implemented with User Behaviour Analyser (UBA). First, whenever a node A wants to send a message to node B, it sends a request to B. Then Node B cast a positive or negative vote according to the credibility of node A. Based on the voting of B, an Acceptance Rate (ACR) of A is calculated. If the Acceptance Rate (ACR) is less than 0.5, then A is marked as a suspicious node and sent for user behaviour analysis. In user behaviour analyzer, all messages either text or media are checked using text and media content filters. All the Bad messages are filtered. Based on the count of messages that have been blocked, a Global Acceptance Rate(GAR) is calculated by taking the average of acceptance rate(ACR), message post rate(MPR), and propagated trust score(PTS). This global acceptance rate is used to exploit the negative links.

3.1. Advantages and Disadvantages of various techniques:

S. No.	Techniques Used	Advantages	Disadvantages
1.	RPC	• Flexible and Exact • Enhance data transmission • Enhance Throughput	• High False Positive Rate • No route restore procedure in case of route corrupt • Neighbor analysis is only used to detect the attack
2.	CAM and PVM	• Detect and eliminate Sybil attack • Throughput increased to 85%	• Time Consuming • Cost-effective
3.	CAM-PVM with MAP	• Prevents Sybil attack • Throughput increased to 95%	• Time Consuming • Cost-effective
4.	Lightweight with energy and frequency	• Improved throughput by 21% of the previous technique.	• Time-consuming
5.	RSS	• Efficient • No data loss	• High end to end delays
6.	RAI-LVT	• Prevent attack by 88%	• Time Consuming

4. Conclusion and Future Scope

WSN, MANET, and OSN are prone to various internal attacks, and Sybil attack is one of the attacks. In this paper, we have first studied what is the Sybil attack and its hazardous effects. After that, we studied various research papers to detect and prevent the Sybil attack. Every paper has some advantage over previous techniques but lack in one way or other for full effectiveness. After studying all the techniques, the author finds Received Signal Strength (RSS) is the most appropriate and efficient technique that can be used in all three networks studied above. RSS prevents any kind of data loss. The detection rate [9] in RSS is 98% and can be improved to 100% in the near future. Also, more work can be done in reducing End to End delays. The information given through this paper will provide a relevant path and make it easy for the researchers to work in this field.

References

[1]. Bindu Rani And Harkesh Sehrawat, “Blackhole Attack Detection And Prevention In Wireless Sensor Networks: A Study” Journal Of Emerging Technologies And Innovative Research (JETIR) March 2018, Volume 5, Issue 3.

[2]Bindu Rani, Harkesh Sehrawat And Vikas Siwach, “Blackhole Attack in Wireless Sensor Network (WSN) using AODV protocol” International Journal Of Advanced Science and Technology(2005-4238)Volume 29-No.4, February 2020.

[3] M. A. Matin And M. M. Islam, “Chapter 1 Overview Of Wireless Sensor Network” IntechOpen, 2012.

[4]. Anamika Pareek And Mayank Sharma, “Detection And Prevention Of Sybil Attack In MANET Using MAC Address” International Journal Of Computer Applications (0975 – 8887) Volume 122 – No.21, July 2015.

[5]. Zhi Yang, Jilong Xue, Xiaoyong Yang, Xiao Wang, And Yafei Dai, “Votetrust: Leveraging Friend Invitation Graph To Defend Against Social Network Sybils” 10.1109/TDSC.2015.2410792, IEEE Transactions On Dependable And Secure Computing.

[6]. Amuthavalli, R., And RS Bhuvaneswaran, "Detection And Prevention Of Sybil Attack In Wireless Sensor Network Employing Random Password Comparison Method," Journal Of Theoretical & Applied Information Technology 67, No. 1, 2014.

[7]. MANJU V C, “Sybil Attack Prevention In Wireless Sensor Network” International Journal Of Computer Networking, Wireless And Mobile Communications (IJCNWMC) ISSN(P): 2250-1568; ISSN(E): 2278-9448 Vol. 4, Issue 2, Apr 2014, 125-132.

[8]. Udaya Suriya Raj Kumar Dhamodharan And Rajamani Vayanaperumal, "Detecting And Preventing Sybil Attacks In Wireless Sensor Networks Using Message Authentication And Passing Method," The Scientific World Journal 2015.

[9]. Roopali Garg, Himika Sharma ”Proposed Lightweight Sybil Attack Detection Technique In MANET” International Journal Of Advanced Research In Electrical, Electronics And Instrumentation Engineering Vol. 3, Issue 5, May 2014.

[10]. Mohsin Mulla And Santosh Sambare, “Efficient Analysis Of Lightweight Sybil Attack Detection Scheme In Mobile Ad Hoc Networks” International Conference On Pervasive Computing (ICPC).

[11]. Dhanalakshmi, T. G., N. Bharathi, And M. Monisha, "Safety Concerns Of Sybil Attack In WSN," In Science Engineering And Management Research (Icsemr), International Conference On, Pp. 1-4, IEEE, 2014.

[12]. Anagha P B, Janitha Krishnan, “Vote Credence: Social Network Sybil Defence By User Behaviour” International Journal Of Science And Research (IJSR) Volume 5 Issue 6, June 2016.