ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Survey on Sybil Attacks and its Defensive Measures

Neha Gahlot[1]

IV SEM M.Tech (S.E), Dept. Of CSE, GECB, Bikaner, India[1]

Abstract: Wireless sensor network are used in many fields now days like military application and ecolological area like flood detection and various other fields like health related. So the security of wsn is important issue. There are some constraints in wsn such as low battery and less memory which can lead to severe attacks in wsn. There are many attacks in wsn one of them is sybill attack. Sybill attack is an attack in which nodes illegally take multiple identities. In this paper we will discuss the taxonomy, classification of sybill attack and there defence mechanism.

Keywords: Sybil Attack, defence, Sensor Networks, Security, peer to peer system.

I. INTRODUCTION

Wireless sensor networks are getting popular these days because of their less expensive solutions to the various real world problems. Their less expensive solutions provide various ways to perform any of military and civilian tasks in any critical condition.

But there is a major obstacle in implementation of security and these are due to lack storage and power resource in wsn.**[3]**.In this paper, we are discussing about most harmful attack in WSN i.e. Sybil attack. In Sybil attack a malicious illegitimately take more than one identity. For example attacker creates several nodes using one physical device.

Doucer described first about the Sybil attack in context of P2P networks. And he also stated that

Redundancy mechanism of distributed storage system could be defeated by it. In this paper we will examine Sybil attack and its defences and further classify the forms Sybil attack and how any attacker can use these forms to compromise any protocol. [2]

II. Classification of SYBIL ATTACK

We will define an attack as Sybil attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. To understand it better we will discuss different forms of Sybil attack .these are as follows:

Direct vs. indirect, fabricated vs. stolen identities, and simultaneity.

1. Direct vs. Indirect Communication

Direct Communication: this a kind of way to perform Sybil attack, in this attack malicious node communicates directly with the legal node. When any legal node is sending radio message to other node then one of the malicious node listen to this message and give reply on the behalf of that node.

Indirect Communication :Indirect communication as its name say there is no direct communication that means the legal or we can say legitimate node can't connect directly with malicious node there is one malicious device between them through which messages are routed.[3]

2. Fabricated vs. Stolen Identities

A new identity could be taken by a fake node through one of the two ways. It can fabricate a new identity, or it can steal an identity from a legitimate node.

Fabricated Identities: In some cases, the attacker creates arbitrary new identities. For example, if a node is identified by the bits like 32 bits of integer value then attacker assign 32 bit value randomly to each node.

Stolen Identities: if an attacker can't fabricate new identity then it will stole an identity. For instance, if the name space is limited so that attacker cannot insert new identity then attacker needs to stole some legitimate identities and this theft remains undetected. [3]

3. Simultaneity

Simultaneous: The attacker participate with all his identities at once .In this a particular hardware identity act as only one identity while circulate one identity at a time so that it appears to be simultaneous participation.

Non-Simultaneous: in non simultaneous attack the identities participate in non simultaneous way that means attacker present a great no. of identities at a time while it act as there is small no. of identities at given time. This is done through a strategy in which when one identity left the network other identity join in place of that identity. The attacker can use different possibilities like one identity can be join or leave multiple times or attacker could use one identity at a time**. [3]**

III. SYBIL ATTACKS IN DIFFERENT FORMS

There are various application affected by Sybil attacks in different areas are described below [1]

1. Routing in a Distributed Peer-to-peer System

In wireless sensor network multipath routing is adopted to increase its performance .In multipath network there are multiple paths present between the nodes throughout its network. This multipath routing increases the performance and efficiency of network, and thus provides better load balancing techniques. However, invalidation of this technique can be easily possible for Sybil attacks. In multipath routing there are multiple paths in which

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

attacker can easily insert a malicious node and route all the messages through that node. It can also affect some other routing algorithms like decentralized object location algorithm, and geographic routing algorithm.

2. Distributed Storage Applications in Peer-to-peer Systems

Duplication and splitting mechanism is generally used in Distributed storage systems. And the mapping of data to their corresponding node is done by using hash function. The mapping function in hash is one- to- many form so attacker can manipulate the values of Sybil identities by replicating the whole data on malicious node .and it will show as data stored on different nodes. By this strategy attacker can easily attack on data for an instance, he can change any of the data value without being identified because he is having all the data copies.

3. Distributed Voting Applications in Peer-to-peer Systems

Any distributed voting aggregation system is vulnerable to Sybil attacks. [1] In distributed voting system different entities are being voted by different identities. It is preassumed that each user have one identity through which they can vote only for one .but the attacker can attack by creating more than one identity then have multiple votes The vote can be of any type like it's used to represent opinion of users positive or negative. The voting system can also be used for assigning ranks to any objects by aggregating votes from the different participants .Attacker can create multiple fake identities and change the majority results. By this way the real opinion of users may changed. Here we need to take an example for better understanding, let's take an example of flipkart's user feedback system, in this reputation of each merchants is decided by users votes .now the attacker can create multiple fake identities and then change merchants reputation using fake votes..

4. Vehicular Ad hoc Networks (VANETs)

A Vehicular Ad-Hoc Network is a technology in which cars are used as nodes to create a network. In this system each car can communicate with other cars or with the roadside base station through signals. These kind of system or network can easily be attacked by any attacker .for example a driver can signal a wrong information everywhere that he is in a traffic jam or that place is in traffic ,so that the other drivers change their route and he can enjoy the less traffic route .

Moreover, the Sybil attack can be life threatening if the fake node or we can say malicious car node drops a wrong message of warning. In VANETs system whenever any accident happens there is a message flashed of slowing speed in car and passed to every nearby vehicle to slow down their speed .but if this wrong warning message is spread all over the vehicles through the provided fake identities then this could create a serious danger for many lives.

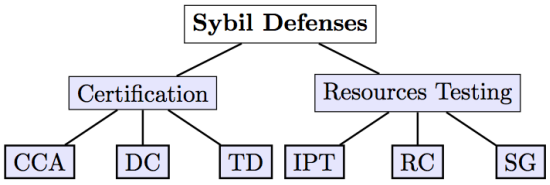
5. Data Aggregation in peer-to-peer Applications

In order to conserve energy sensor network use some aggregation protocols to aggregate the readings of sensors. But this situation is easily vulnerable to attacks .the attacker can easily inject some malicious nodes into the network and that node can alter the readings .by this the aggregated value is changed and attacker could manipulate these values according to their needs.

6. Sock puppets in Online review Forums

In online review forums, to impress the buyers for the products, that it is a good buy, they use a plan to duplicate the identities and pretending that they are different people. This is all done to cheat people and make them believe that this is the most wanted product in the market, so that the value of product increased in front of buyers. In the same forum, different online entities which belong to the same person are referred as „sock puppets." Note that sock puppet does not belong to Sybil attack, since online discussion forums are not peer-to-peer systems. However, because sock puppets have several features similar to Sybil attacks, we want to mention them.

IV. FUNCTIONAL CLASSIFICATION OF SYBIL DEFENCES



In this paper we will discuss the defences are classified into two broad categories: trusted certification and resource testing categories, as shown in Figure. Among the schemes in the trusted certification category, we survey works that use a centralized certification authority (CCA), decentralized cryptographic primitives, or trusted devices. Among works that use resource testing, we are particularly interested in works that use IP testing, cost recurrence, and social graphs [4].

1. Defenses Using Trusted Certification

The trusted certification approach is most important approach in Sybil defences. In this approach, centralised authority check whether the identities assigned to each node is legitimate or not by matching it with the credentials that are previously assigned. The Credentials that are previously assigned may consists of cryptographic keys, random strings that are generated from one time password generator. Or credentials may also contain digital certificates assigned by centralized authority.

a. Centralized Certification Authority

Sybil attack can be eliminated by only method that is Centralized trusted certification. There is some discussion about the use of centralized certification authorities .CCA is used for credential generation, verification and assignment in concern of P2P system. For example public key cryptography is mostly used in network, the authenticity of these keys is ensured by certificates that are assigned to the users by CCA.

b. Cryptographic Primitives

These cryptographic primitives makes harder for attacker to attack on any network by encouraging only legal nodes to participate in the network. Through this cryptographic primitive we are trying to exploit public keys to ensure

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

that when the users connect with each other are authenticated correctly before the connection or not. Generally, many of the protocols use the certification system for legitimate user to enter into network; hence cryptographic primitive's helps such protocol to complete their operation successfully.

c. Trusted Devices

Trusted certification and trusted devices are basically similar, trusted devices are suggested by some researchers to use to store some important informations like certificates, keys and it must be harder to reach to anybody because of their price. So that Sybil attackers couldn't easily impersonate the identity. Examples of such mechanisms are proposed by NEWSOME.

2. Defenses Using Resource Testing

The basic approach used in resource testing to defend from Sybil attack is to check whether set the of identities associated with users using enough resources in comparison to the identities or they are using more. The resources here are computation power, bandwidth, memory, IP address, or even trust credentials.

In this approach, the techniques applied which tries to limit the no. of Sybil identities in a particular place without any defence .but the limited no. of Sybil identities are also harmful for the security of system. To understand better, let's take an example of random system .In these system two nodes depend on one circuit and according to the approach the Sybil identities should be limited .so according to approximate calculation only 1% user can out vote legitimate nodes. So by this technique it is clear that it mitigate the Sybil attack not totally eliminates it.

a. IP Testing

In IP testing technique the IP address is traced to get the location of that particular peer and then their activities are checked and if some suspected activities are noticed from same location then there must be a Sybil identity present. But in this technique the IP address tracing is not cheap, it is an expensive procedure. For example, Freedman and Morris [11] introduced Tarzan, in which IP addresses of peers are tested based on their geographic location in a particular autonomous system. Similar results were introduced by Cornelli et al. [12].

The main point to be noticed is that IP address tracing is not easy in a wide geographical areas. And if node is compromised which is comes under a particular administration but originally present in some other system then this technique is totally useless.

b. Recurring Cost

Recurring cost is charged against work for defending against Sybil attack .for this computational puzzle like CAPTCHA is suggested as solutions. There are various other solutions phone number verification and email verification that is used by Google during registration of any social networking site. But the cost based scheme doesn't work well as the same thing happens in IP testing.

The CAPTCHA like puzzles can be solved by Sybil attacker. Attacker post their captcha on sites controlled by them, so that the user solve that captacha for them and they get easy access to the sites. System Specific Features-Location / Position Verification. It is used in defending wireless adhoc networks. This method use Sybil detection method ,in this method the communication rate of the channels are matched and if there is conflict in the channel rate then there must be a Sybil identity. There is a central authority whose work is to record the rate of each identity and if there is any conflict occur in channel rate then Sybil identity will be detected .Paper [10] proposed a Sybil detection method by monitoring the neighbours‟ channel conflict rate.

4. Social Network Based Techniques to Defend Sybil Attacks**.**

Here the Sybil attacks detected based on a unique

Structure: although attackers can create plenty of Sybil identities, and further establish several links among them; the total number of links between the Sybil and the honest users is limited, since the trust relationship on a social network is built based on the trust relationship among real people.

a. Sybil Guard and Sybil Limit

Sybil Guard [5] and Sybil Limit [6] are two famous Sybil defenses that use social networks. Here we will discuss Sybil Guard only. Sybil Guard defines two terms, 1 a trusted path, 2. A trusted node Sybil Guard also assumes that there is a known trusted node. From this trusted node, there are „K‟ random paths with a fixed length. For the ease of description, we call these paths verifiers. From a suspect node, Sybil Guard also sends „k‟ random paths. If a path encounters a verifier once, then we call the path „been verified once. If a path has been Verified „S‟ times, then the path is a trusted path. When the most of the paths of a suspect node are trusted paths, the suspect node will be treated as a trusted node; otherwise the node is a Sybil. Sybil Guard suffers from high false negatives, as each attack edge may introduce $O(\sqrt{n} \log n)$ Sybil nodes without being detected. The advanced version of Sybil Guard, Sybil Limit, reduces this value to O(log n), to detect the Sybil region with Sybil Guard or Sybil Limit, all the suspect nodes in the social graph need to be tested.

b. Sybil Infer

Sybil Infer [7], a centralized Sybil defense algorithm, leverages a Bayesian inference approach that assigns a Sybil probability, indicating the degree of certainty, to each node in the network. It achieves low false negatives at the cost of high computation overhead. The overall time complexity of Sybil Infer is O(|V |2 log |V |), where V is the set of vertices in the social graph. In the evaluation Sybil Infer handled networks with up to 30K nodes, which is much smaller than the size of regular online social networks.

c. Gate Keeper

Gate keeper [8], a decentralized protocol that performs Sybil-resilient node admission control mainly based on a social network. Gatekeeper can admit most honest nodes while limiting the number of Sybil's admitted per attack edge toO(log k), where k is the number of attack edges. Gate Keeper scheme that heavily relies on the assumption that the social networks are random expander. This is a strong assumption which has not been validated by

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

previous research. Our evaluation shows that GateKeeper suffers from high false positive and negative rates and cannot effectively identify Sybil nodes on the real-world asymmetric social topologies.

d. Sybil Defender

Sybil Defender [9], a Sybil defence mechanism that Leverages the network topologies to defend against Sybil attacks in social networks. Based on performing a minimum number of random walks within the social graphs, Sybil Defender is most efficient and it is scalable to large social networks. Sybil Defender can effectively identify the Sybil nodes and detect the Sybil community around a Sybil identity, even when the number of Sybil nodes introduced by each attack edge is close to the theoretically detectable lower bound. Sybil Defender consists of two components: a Sybil node identification algorithm, a Sybil group around that Sybil node detection algorithm.

V. CONCLUSION

In this paper we have discussed about the types of Sybil attacks according different application .we have also discussed some techniques to defend against Sybil attack.

REFERENCES

[1] Rakesh G.V,Shanta Rangaswamy, Vinay Hegde,Shobha G ,"A survey of techniques to defend against Sybil attacks in social networks", in International Journal Of Advance Research in computer and Communication Engineering,Vol. 3,Issue 5,May 2014

[2] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack sensor networks: analysis & defenses," in Proc. of ACM IPSN, 2004 pp. 259–268.

[3] John Paul Walters ,Zhenjiang liang,weisong shi, and vipin choudhary. A survey :wireless sensor network. In security in distributed ,grid and pervasive computing.2006

[4] Aziz Mohaisen and Joongheon Kim"sybil attack and defences : a survey" in Smart Computing Review, vol. 3, no. 6, December 2013

[5] H. Yu, M. Kaminsky, P. Gibbons, and A. Flaxman, "Sybilguard: defending against sybil attacks via social networks," in Proc. Of ACM SIGCOMM, vol. 36, no. 4, 2006, pp. 267–278

[6] H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao "Sybillimit: a nearoptimal social network defense against sybil attacks," in Proc. Of IEEE Symposium on Security and Privacy, 2008, pp. 3–17.

[7] G. Danezis and P. Mit. Sybilinfer: Detecting sybil nodes using social networks. In NDSS, 2009.

[8] N. Tran, J. Li, L. Subramanian, and S. S.M. Chow. Optimal sybilresilientnode admission control. In IEEE INFOCOM, 2011.

[9] SybilDefender: Defend Against Sybil Attacks in Large Social Networks Wei Wei∗, Fengyuan Xu∗, Chiu C. Tan†, Qun Li The College of William and Mary, †Temple University.

[10] C. ZHENG and D. S. GILBERT, "Thwarting sybil attacks and malicious disruption in wireless networks," http://www.comp.nus.edu.sg/ zheng-10/talk/grp-2012- 09-14-paperv3.pdf.

[11] M. J. Freedman, R. Morris, ―Tarzan: a peer-to-peer anonymizing network layer,‖ in Proc. of ACM CCS, pp. 193-206, 2002. Article (CrossRef Link)

[12] F. Cornelli, E. Damiani, S. D. C. di Vimercati, S. Paraboschi, P. Samarati, ―Choosing reputable servants in a P2P network,‖ in Proc. of ACM WWW, pp. 376- 386, 2002.