ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (11-17), Month: July - September 2016, Available at: www.researchpublish.com

Sybil Attack

Neelam Yadav[1], Heena Mehta[2]

[1] (PG Student): Dept. of Computer Science & Engineering, World College of Technology and Management.
[2]Assistant Professor: Dept. of Computer Science & Engineering, World College of Technology and Management.

Abstract: **The survey and classification of the different security attacks in structured peer-to-peer (P2P) overlay networks can be useful to computer system designers, programmers, administrators, and users. In this research, we attempt to provide taxonomy of structured P2P overlay networks security attacks. Which ensures the existing network are still a way from the security and their safe working. We have specially focused on the way these attacks can arise at each level of the network. Moreover, We observed that most of the existing systems such as Content Addressable Network (CAN), Chord , Pastry, Tapestry, Kademlia, and Viceroy suffer from threats and vulnerability which lead to disrupt and corrupt their functioning. The idea of this survey was conceived when we were considering how to secure structured P2P overlay networks from security attacks without a central coordination. We are convinced that knowing how systems have failed can help us to build systems that resist to failure. This paper provides an overview of different categories of hierarchical P2P systems and took a major security attacks threatening the function of structured P2P overlay networks. We classified these attacks into two main groups: general network attacks and specific structured P2P network attacks. Both networks are secured but General network are less secured as compared to Specified structured network because of their decentralized nature. For this various Security goals are discussed which provide services how to secure the network at different level. At each level attack is detected and solved at same time by this the data can be secured and safely used. This paper provides a way to handle that problem before it harms to the network. By this the data is made secured from the hacking. I hope that this survey constitutes a good help for security of the network and who's want to work on this area of research. In light of this study we can affirm that existing structure P2P can be safely utilized and secured from attack.**

***Keywords*: P2P, Structured P2P overlay network, security, CAN, classification.**

I. INTRODUCTION

A Sybil attack is one in which a malicious node on a network illegitimately claims to be several different nodes simultaneously. Many distributed applications and everyday services assume each participating entity controls exactly one identity. When this assumption is unverifiable the service is subject to attack. In a large-scale peer-to-peer system, a direct connection between each pair of nodes is impossible, therefore, the nodes which are participating usually create networks, and a message is transmitted from one node to another via the relay operations of multiple intermediary nodes. In this paper, we investigate the Sybil attack, a dangerous attack in distributed peer-to-peer networks[1]. Almost distributed peer-to-peer systems are based on a common assumption that each participating entity controls exactly one identity. However, whenever the assumption cannot be fulfilled, the system lead to Sybil attacks. In a Sybil attack, an adversary creates a large number of false/fake/Duplicate identities (Sybil identities), and since all Sybil identities are controlled by the adversary, It can maliciously introduce a considerable number of false opinions into the system, and convert it, by making decisions benefiting system itself.

A Peer to Peer (P2P) network is a distributed network composed of a large number of distributed, heterogeneous, and independent peers. P2P networks provide an alternative to the traditional client-server communication model in which a node in a P2P network can act as a server and a client at the same time.

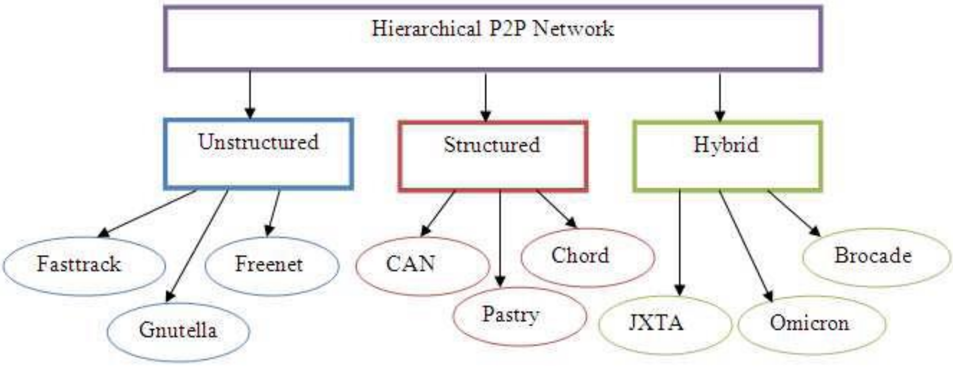

Fig. 1 Hierarchial P2P network

The P2P computing provides properties like no central point of failure and no service bottlenecks by decentralizing the service among participating nodes. In recent years many research work have been done and are still in progress to improve their robustness, security and scalability

II. SECURITY ATTACKS IN STRUCTURED P2P OVERLAY NETWORKS

2.1. General Network Attacks

1) DoS and DDoS

With time and as the internet gets more and more used as a communication channel, Denial of Service (DoS) and Distributed Denial of Service (DDos) become more popular than ever. A DoS attack and DDoS attack are characterized byan explicit attempt by attackers to prevent legitimate users of a service from using that service, in other words, this is an attack which causes a service to stop functioning or an attack that causes the loss of service. In DoS attack, attacker utilizes reasonable service requests to drain the resources of a target host. However, in DDoS attack attacker exploits considerable amount of distributed hosts to launch the attack to the target.

2) Worm propagation

Worms pose one of the biggest threats to the internet. Currently, worms such as Code Red or Nimda are capable of infecting hundreds of thousands of hosts within hours and no doubt that better engineered worms would be able to infect to reach the same result in a matter of seconds.

3) Man in the middle

The man in the middle attack is a form of active eavesdropping in which an attacker inserts himself between two other nodes in the network, makes independent connections, and relays messages between them. The attacker makes the two nodes believes that they are talking directly to each other when in fact all communication passes through him. He can achieve this by inserting, dropping, or retransmitting previous messages in the data stream. In this case, the attacker can modify messages, insert fake information, and in the worst case assume the identity of either node or both to launch a denial of service.

4) Botnets

One of the most significant threats to the internet today is the threat of botnets, which are networks of compromised machines under the control of an attacker. A botnet produces very significant threats to structured P2P networks. Compared to other internet malware, botnets are different from traditional discrete infections in that they act as a coordinated attacking group.

5) Eavesdropping attack

Eavesdropping is another type of attack on networks. Attackers can gain access to data within a network and eavesdrop the traffic. One of the biggest security problems faced by users is the ability of attackers (eavesdroppers) to monitor networks, that is leads to several problems such as sniff passwords and keys, get MAC address, get IP address, and capture data to eventually cause the network to crash or even become corrupted. The first step in preventing eavesdropping attack is to use a strong physical security, and the next step is to use strong encryption services that are based on cryptography.

6) Masquerade attack

Masquerade attack is a type of attack in which one system entity illegitimately poses as another entity to gain access to confidential systems. This means to hide one's true identity on the network to create a spoofed identity. Masquerade attacks are extremely serious; they can occur in several different ways, they may get access to a legitimate user's account either by stealing a victim's password, or through IP address[6]. A common method to limit this type of attack is to filter incoming packets that appear to come from an internal IP address and filter outgoing packets that appear to originate from an invalid local IP address.

2.2. Specific Structured P2P network attack

1) Assigning node IDs attack

Before joining the network, every peer must usually generate a user identifier. These user identifiers uniquely identify node in a P2P networks. However, the assignment of IDs is usually not controlled enough. This allows malicious users to perform different types of attacks such as Sybil attack and Id mapping attack.

- ***Sybil attack***

Due to the open nature of the Structured P2P network a single malicious user can create multiple fake identities and pretend to be multiple, distinct physical node in the system. Such attack is known as Sybil attack. In this case, malicious node can compromise the network by generating and controlling large numbers of fake identities. It can attack several protocols such as distributed storage to defeat replication and fragmentation mechanisms, and routing.

- ***ID mapping Attack***

In structured P2P overlay networks; there is a uniform random distribution of node identities (Ids). This random distribution allows an attacker to obtain some particular identifier and gain a strategic position on the overlay network to eventually gain control over certain resources.

- ***Incorrect routing update***

The major issue of the DHT based networks such as Chord, Pastery, and Tapestry was the creation of the routing table. Each node creates their routing table by consulting other nodes. A malicious user could corrupt the routing tables of others nodes by sending them invalid updates to cause misdirect queries to inappropriate nodes, or to non-existent nodes[9]. Different solutions are developed for this kind of problem such as impose certain requirements

2) Routing attack

According to the function of DHT algorithm each node in the overlay maintains a routing table which guarantee the look up and mapping of the keys. Routing attacks are performed by exploiting the weaknesses in the routing mechanisms. In this section, we describe the most important routing level attacks faced in structured P2P networks.

- ***Incorrect routing update***

The major issue of the DHT based networks such as Chord, Pastery, and Tapestry was the creation of the routing table. Each node creates their routing table by consulting other nodes. A malicious user could corrupt the routing tables of others nodes by sending them invalid u-

- ***Incorrect lookup routing***

Lookups for keys in Structured P2P overlay networks are performed by routing queries through a series of nodes. Each of these nodes uses a local routing table to forward the query toward the node responsible for the key. This mechanism is used to store, retrieve, replicate, and authenticate the data. Since the malicious node could corrupt this mechanism through routing updates system; it could forward messages to an incorrect or non-existent node.

- ***Eclipse attack***

Due to the fact that each node in the network maintains overlay links to a set of neighbor nodes and each node uses these links to perform a lookup from its neighbors, an attacker can control a significant part of overlay network by controlling a large part of the neighbors of correct nodes. This attack is known as Eclipse attack using pdates to cause misdirect queries to map.

- ***Identity theft attack***

In P2P overlay networks, each node of the structured P2P overlay network knows only a small fraction of other nodes. A node wanting to deliver a message to the root node of some key just had to trust that the other nodes will route the message to the correct root node. However, malicious user can exploit this trust to launch identity theft attack propriate nodes, or to non-existent nodes[9].

- ***Churn attack***

Structured P2P overlay networks are widely used to deploy services. This characteristic makes such system attractive to thousands or millions of users and at the same time vulnerable to the phenomena of churn. The independent arrival and departure of thousands or millions of peers creates a collective effect called churn. An attacker could exploit this attack by generation peer joining and leaving the network fast enough to corrupt the best function of the network

2.3. Review of Security Issues, Vulnerabilities And

Challenges

Transferring our data to additional organization is not secure, as there is a lot of risk from insider of company or as well as outsider of company though for this comprehensive understanding of security issues need to be understood and must resolve those issues .

Rakesh G.V, Shanta Rangaswamy,Vinay Hegde,Shoba G et.al.[1] Most peer-to-peer systems are vulnerable to Sybil attacks. The Sybil attack is an attack where in an adversary creates multiple Duplicate or False identities to compromise the running of the system. By including false information by the Duplicated entities, an adversary can mislead a system into making decisions benefiting. For example, in a distributed review system, an adversary can easily change the overall review of an option by providing plenty of false praise, the option through these fake identities. Defending against Sybil attacks is quite challenging. In this paper, we summarize the existing Sybil defense techniques; we first group the Sybil defense methods, mainly according to their type, and then divide the methods by their approaches.

Haifeng Yu Michael Kaminsky Phillip B. Gibbons Abraham Flaxman et.al.[2] Peer-to-peer and other decentralized, distributed systems are known to be particularly vulnerable to sybil attacks. In a sybil attack, a malicious user obtains multiple fake identities and pretends to be multiple, distinct nodes in the system. By controlling a large fraction of the nodes in the system, the malicious user is able to “out vote” the honest users in collaborative tasks such as Byzantine failure defenses. This paper presents SybilGuard, a novel protocol for limiting the corruptive influences of sybil attacks. Our protocol is based on the “social network” among user identities, where an edge between two identities indicates a human-established trust relationship. Malicious users can create many identities but few trust relationships. Thus, there is a disproportionately-small “cut” in the graph between the sybil nodes and the honest nodes. SybilGuard exploits this property to bound the number of identities a malicious user can create. We show the effectiveness of SybilGuard both analytically and experimentally.

R. AMUTHAVALLI, DR. R. S. BHUVANESWARAN el.at.[3] Security is imperative for some Sensor Network Applications. An especially unsafe assault against sensor and impromptu systems is known as the Sybil attack, where a node illegitimately asserts numerous characters. In this type of attack a legal node is converted into a Sybil node which is a replica node with a different personality but using a similar ID. This leads to data leakage which causes data integrity violations. In existing research, nodes can detect the suspect nodes by checking the nodes in its neighborhood i.e within a given range. The neighbor nodes exchange information about each other and detect the Sybil node as it provides misleading information. The Sybil nodes are not detected directly by checking the ID or other node related information. In this paper, a Random Password Comparison [RPC] method is proposed that facilitates deployment and control of the position of node thereby preventing the Sybil attack. The RPC method is dynamic and accurate in detecting the Sybil attack. This method improves data transmission in the network and will also increase the throughput.

Roopali Garg , Himika Sharma el.at.[4] In Sybil attack, attackers use several identities at a time or they take-off identity of some trustworthy node present in the network. This attack can create lots of misinterpretation in the network like decrease the trust of legitimate node by using their identities, disturbs the routing of packets so that they cannot reach to its desired destination, and many more. Like this it disturb the communication among the nodes present in the network. Sybil attack is very much destructive for mobile ad-hoc network. In this research, we implemented the Lightweight Sybil Attack Detection technique which is used to detect the Sybil nodes in the network and also discussed the proposed work with implementation which is used to improve the existing Lightweight technique. Simulation tool used for the implementation is MATLAB.

Himadri Nath Saha , Dr. Debika Bhattacharyya , Dr. P. K.Banerjee el.at[5] Sybil attack is a serious threat for today’s wireless adhoc networks. In this attack a single node impersonates several other nodes using various malicious means. In this paper we attempt to provide a hybrid solution using a combination of two already proposed methods. According to this newly proposed method the total network will be dynamically divided into several subgroups, as more and more nodes will enter the network. Each subgroup will be under the super vision of a single node, a central authority. Each subgroup will also contain RSSI detector nodes.

Mina Rahbari and Mohammad Ali Jabreil Jamali el.at.[6] Vehicular communications play a substantial role in providing safety transportation by means of safety message exchange. Researchers have proposed several solutions for securing safety messages. Protocols based on a fixed key infrastructure are more efficient in implementation and maintain stronger security in comparison with dynamic structures. The purpose of this paper present a method based on a fixed key infrastructure for detection impersonation attack, in other words, Sybil attack, in the vehicular ad hoc network. This attack, puts a great impact on performance of the network. The proposed method, using an cryptography mechanism to detection Sybil attack. Finally, using Mat lab simulator the results of this approach are reviewed, This method it has low delay for detection Sybil attack, because most operations are done in Certification Authority, so this proposed schema is a efficient method for detection Sybil attack.

Anuja Motarwar, Prof. Amresh Kumar el.at.[7] As the technology improves the method of communication and reduces the network overhead it also opens a wide spectrum for attacker to break the security. As wireless communication happens through open air, it also increases possibility of fetching the information from air medium using sniffing software tools. A particularly harmful attack against sensor networks is known as the Sybil attack, where a node illegitimately claims multiple identities and simultaneously uses those identities in the network. In this paper we analyze fake identity in network which is created by Sybil attack by detecting its source. Analysis have found some solution that include the communication among the nodes of cluster and analyze the results in different scenarios like fake sender detection, fake receiver blocking, node to node secure connection and packet acceptance and rejection process.

III. CONCLUSION

The idea of this survey was conceived when we were considering how to secure structured P2P overlay networks from security attacks without a central coordination. We are convinced that knowing how systems have failed can help us to build systems that resist to failure. This paper provides an overview of different categories of hierarchical P2P systems and took a major security attacks threatening the function of structured P2P overlay networks. We classified these attacks into two main groups: general network attacks and specific structured P2P network attacks. Finally, we close this survey with a discussion of the different links between attacks and we confirm that ensuring that a structured P2P overlay network will be sufficient and suitable involves the balancing of many factors such as trust, privacy and security. In light of this study, we can affirm that existing structured P2P overlay networks are still a way from a safe utilization. Thus, the development of appropriate security measures seems to be a mandatory.

LITERATURE REFERENCE 13

Problem Discussed: faulty and hostile remote computing element

Technique Used: trusted agency certified identities

Model/Tool/Purposed: Yes

Large-scale peer-to-peer systems face security threats from faulty or hostile remote computing elements. To resist these threats, many such systems employ redundancy. However, if a single faulty entity can present multiple identities, it can control a substantial fraction of the system, thereby undermining this redundancy. One approach to preventing these “Sybil attacks” is to have a trusted agency certify identities. This paper shows that, without a logically centralized authority, Sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities.

LITERATURE SURVEY 14

Problem Discussed: Location privacy

Technique Used: Footprint

Model/Tool/Purposed: Yes

This paper work not only able to detect Sybil attack but also preserve location privacy of the node. In this detection scheme trajectory of vehicle is used while still preserving anonymity and location privacy of vehicle. In this scheme when a vehicle comes into range of a road side unit(RSU) it requests an authorized message from RSU and message is issued by RSU for that vehicle. This authorized message is a proof that this particular vehicle is present at that particular time in its range. Authorized messages can be used to use to identify a vehicle as message would be different at different location.

LITERATURE REFERENCE 17

Problem Discussed: Defending agaist Sybil attack

Technique Used: computational puzzles

Model/Tool/Purposed: Yes

The problem of defending against Sybil attacks using computational puzzles. A fundamental difficulty in such defenses is enforcing that puzzle solutions not be reused by attackers over time. We propose a fully decentralized scheme to enforce this by continually distributing locally generated challenges that are then incorporated into the puzzle solutions.

LITERATURE REFERENCE 18

Problem Discussed: vulnerable to Sybil attack

Technique Used: Sybil Guard

Model/Tool/Purposed: Yes

This paper presents Sybil Guard, a novel protocol for limiting the corruptive influences of Sybil attacks. Our protocol is based on the "social network "among user identities, where an edge between two identities indicates a human-established trust relationship. Malicious users can create many identities but few trust relationships. Thus, there is a disproportionately-small "cut" in the graph between the Sybil nodes and the honest nodes. Sybil Guard exploits this property to bind the number of identities a malicious user can create. We show the effectiveness of Sybil Guard both analytically and experimentally.

REFERENCES

[1] Rakesh G.V, Shanta Rangaswamy , Vinay Hegde , Shoba G, " A Survey of Techniques to Defend Against Sybil Attacks in Social Networks", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 5, May 2014.

[2] Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons Abraham Flaxman, "SybilGuard: Defending Against Sybil Attacks via Social Networks", SIGCOMM'06, Pisa, Italy, September 11–15, 2006.

[3] R. Amuthavalli, Dr. R. S. Bhuvaneswaran, "Detection and Prevention of Sybil Attack In Wireless Sensor Network Employing Random Password Comparison Method", Journal of Theoretical and Applied Information Technology 10th. Vol. 67 No.1, September 2014.

[4] Roopali Garg , Himika Sharma, " Proposed Lightweight Sybil Attack Detection Technique in MANET", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 5, May 2014.

[5] Himadri Nath Saha, Dr. Debika Bhattacharyya, Dr. P. K.Banerjee, "Semi-Centralized Multi-Authenticated RSSI Based Solution to Sybil Attack", International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004) 338 Volume 1, Issue 4, December 2010.

[6] Mina Rahbari and Mohammad Ali Jabreil Jamali, "Efficient Detection Of Sybil Attack Based On Cryptography In VANET", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.

[7] Anuja Motarwar, Prof. Amresh Kumar, "Study on Detection of Sybil Attack in Wireless Sensor Network", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 12, December 2013.

[8] K. Kayalvizhi N. Senthilkumar, G. Arulkumaran, "Detecting Sybil Attack by Using Received Signal Strength in Manets ", (IJIRSE) International Journal of Innovative Research in Science & Engineering ISSN (Online) 2347-3207

[9] Muruganandam1 , R. Anitha, "Passive Adhoc Identity for Sybil Attack Detection Using NDD Algorithm", International Conference on Computing and Intelligence Systems Volume: 04, Special Issue: March 2015.

[10] Byung Kwan Lee , EunHee Jeong and Ina Jung, "A DTSA (Detection Technique against a Sybil Attack) Protocol using SKC (Session Key based Certificate) on VANET", International Journal of Security and Its Applications Vol. 7, No. 3, May, 2013

[11] Bo Yu, Chang-Zhong Xu, Bin Xiao, "Detecting Sybil Attacks in VANETs", In: Journal of Parallel and Distributed Computing 73.6, pp. 746 –756, 2013.

[12] W. Chang, J. Wu, "A survey of Sybil attack in Networks", .Sensor Networks for Sustainable Development, CRC Press.

[13] Douceur, J. R. 2002. The Sybil attack, In Proceedings of the International Workshop on Peerto-Peer Systems (IPTPS), Springer-Verlag[14] Shan Chang, Yong Qi, Hongzi Zhu,Jizhong Zhao, Xuemin(Sherman) Shen, "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks", Parallel and Distributed Systems, IEEE Transactions on, vol. 23. no. 6, 2012, pp. 1103-1114; DOI 10.1109/tpds.2011.263.

[14] Castro, Druschel, P., Ganesh, A., Rowstron, A., and Wallach, D. S. 2002. Secure routing for structured peerto-peer overlay networks. In Proceedings of 5th ACM Symposium on OSDI.

[15] Levine, B. N., Shields, C. and Margolin. N. B. 2006, A survey of solutions to the sybil attack.Tech report, University of Massachusetts, Amherst.

[16] Borisov. N, 2006. Computational puzzles as sybil defenses, In Proceedings of the 6th IEEE International Conference on Peer-to-Peer Computing, IEEE Computer Society.

[17] Yu, H., Kaminsky, M., Gibbons, P. B. and Flaxman, A. 2006. Sybilguard: defending against sybil attacks via social networks, In Proceedings of the ACM SIGCOMM Conference