Volume 6, Issue 1, January 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Survey on the Sybil Attack in Peer to Peer Wireless Sensor Network

Reshma Dafade, Prof. Riya Qureshi
Department of computer science & Engineering, Ballarpur Institute of Technology, Ballarpur
Gondawana University, Maharashtra, India

Abstract— Sybil attack is one of the most challenging problems that plague current decentralized Peer-to-Peer(P2P)systems. In Sybil attack, a single malicious user creates multiple peer identities known as Sybil. These Sybil are employed to target honest peers and hence subvert the system. 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

Keywords— Sybil Attack, P2P Networks, trust, Social Network, Wireless Sensor Network

I. INTRODUCTION

A Sybil attack [2] 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. 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, Peers can collude and do all sorts of malicious activities in the open-access distributed systems. These malicious behaviours lead to service quality degradation and monetary loss among business partners. Peers are vulnerable to exploitation, due to the open and near-zero cost of creating new identities. The peer identities are then utilized to influence the behaviour of the system. However, if a single defective entity can present multiple identities, it can control a substantial fraction of the system, thereby undermining the redundancy. The number of identities that an attacker can generate depends on the attacker's resources such as bandwidth, memory, and computational power.
The goal of trust systems is to ensure that honest peers are accurately identified as trustworthy and Sybil peers as untrustworthy. To unify terminology, we call all identities created by malicious users as Sybil peers.

II. PROPOSED METHODS TO DEFEND SYBIL ATTACKS

There are many methods proposed to control the Sybil attacks are as follows.

A. Sybil Node Detection Algorithm

The Sybil attack was first described by Douceur in the context of peer-to-peer networks [2]. He pointed out that it could defeat the redundancy mechanisms of distributed storage systems. Karlof and Wagner noted that the Sybil attack also poses a threat to routing mechanisms in sensor networks [3].
Douceur observes that the Sybil attack can defeat replication and fragmentation mechanisms in peer-to-peer storage systems [2].

B. Trusted Certification

Sybil attacks can be avoided by using trusted certification. In this method central authority, they can verify the validity of each user, and further issues a certification for the honest one. In real world, such certification can be a special hardware device [4] or a digital number [5], [6].Before a participant joins a peer-to-peer system, provides votes, and to obtains services from the system, his identity must first be verified. For example, when we are applying for a bank atm card, we need to give our social security number for verification.

Centralized trusted certification methods are often implemented by asymmetric (such as public/private keys) Cryptography.

They assumed that each node shares a unique symmetric key with a trusted centralized base station. After checking the validity of each other ,a pair of nodes can establish a shared key. During data transmission between adjacent nodes, they can use the key for mutual authentication and validation, and can also encrypt the data.

Problems with Trusted Certifications

The problems associated with the central authority-based methods, as follows:

a) Single point of attack. In these schemes, the central authority can easily become a target.

b) Performance bottleneck. If many users access a central authority simultaneously, the central authority may fail.

c) Communication cost. In this type of method, the authority should be required during the data transmission.

C. Position Verification

Another promising approach to defending against the Sybil attack is position verification. Here we assume that the sensor network is immobile once deployed. In this approach, the network verifies the physical position of each node. Sybil nodes can be detected using this approach because they will appear to be at exactly the same position as the malicious node that generates them. While there has been research on automatic location determination [7, 16], it remains an open research question how to securely verify a node's exact position. Such a method may be difficult to find, but researchers have proposed methods to securely verify that a node is within a region [18]. By placing a limit on the density of the network, in-region verification can be used to tightly bound the number of Sybil identities that a malicious node can create.

D. 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.

1) Sybil Defender: Sybil Defender[1], 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.

2) Sybil Guard and Sybil Limit: Sybil Guard [8], and Sybil Limit [9] are two famous Sybil defences that use social networks. we will only introduce Sybil Guard. Sybil Guard defines two terms, 1 a trusted path, 2. A trusted node. There is similarly, for breaking the symmetric data constriction, 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.

III. PROBLEM FORMULATION

A. Note that a mobile attacker may be able to present several identities by being verified as one identity at one location, and then moving to a different location and being verified as a different identity as[7,16]. To defeat this type of attack, all nodes' positions could be verified simultaneously. Alternatively, given an upper bound on the attacker's mobility, it would only be necessary to test the nodes within a certain range simultaneously.

B. The resources proposed by Douceur[2] to use for this purpose are computation, storage, and communication. Computation and storage are unsuitable for wireless sensor networks, because the attacker may be using a physical device with several orders of magnitude more computation and storage ability than a resource starved sensor node.

C. SybilGuard[8] and SybilLimit[9] both rely on the assumption that social networks are fast mixing (explained later), and the number of attack edges is limited. To identify sybil nodes, the schemes make use of random routes, a special kind of random walks in which each node uses a precomputed random permutation as a one-to-one mapping from incoming edges to outgoing edges. SybilGurad suffers from high false negatives, as each attack edge may introduce $O(\sqrt{n} \log n)$ sybil nodes without being detected. The improved version of SybilGuard, SybilLimit, reduces this value to O(log n), which is still larger than the proved lower bound $\Omega(1)$ [19] by a log n factor. Moreover, to detect the sybil region with SybilGuard or SybilLimit, all the suspect nodes in the social graph need to be tested.

D. Problem with Sybil Defender[1] the survey results of our Facebook application show that the assumption made by previous work that all the relationships in social networks are trusted does not apply to online social networks, and it is feasible to limit the number of attack edges in online social networks by relationship rating.

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

IV. OBJECTIVE

Defending against Sybil attack is quite a challenging task. A peer can pretend to be trusted with a hidden motive. The peer can pollute the system with bogus information, which interferes with genuine business transactions and functioning of the systems [20]. This must be counter prevented to protect the honest peers.

A) The link between an honest peer and a Sybil peer is known as an attack edge. As each edge involved resembles a human-established trust, it is difficult for the adversary to introduce an excessive number of attack edges.
B) Sybil attack makes use of social networks to eliminate Sybil attack, and the findings are based on preventing Sybil identities.

V. PROPOSED METHODOLOGY

We present a distributed structured approach to Sybil attack. This is derived from the fact that our approach is based on the neighbour similarity trust relationship among the neighbour peers. Given a P2P e-commerce trust relationship based on interest, the transactions among peers are flexible as each peer can decide to trade with another peer any time.
Our contribution in this paper is threefold:

We propose SybilTrust that can identify and protect honest peers from Sybil attack. The Sybil peers can have their trust canceled and dismissed from a group

Based on the group infrastructure in P2P e-commerce, each neighbor is connected to the peers by the success of the transactions it makes or the trust evaluation level. A peer can only be recognized as a neighbor depending on whether or not trust level is sustained over a threshold value.

SybilTrust enables neighbor peers to carry recommendation identifiers among the peers in a group. This ensures that the group detection algorithms to identify Sybil attack peers to be efficient and scalable in large P2P e-commerce networks.

VI. CONCLUSIONS

However, most of the peer-to-peer systems are vulnerable to Sybil attacks. In this paper, we have discussed the important kinds of Sybil attacks that can be applied on various application domains. We presented SybilTrust, a defense against Sybil attack in P2P e-commerce. Compared to other approaches, our approach is based on neighborhood similarity trust in a group P2P e-commerce community.

ACKNOWLEDGMENT

I would like to thank Department of Computer Science & Engineering, Ballarpur Institute of Technology, Ballarpur for providing infrastructure and guidance to understand Sybil Attack In P2P wireless Sensor Network.

REFERENCES

[1] *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
[2] J. R. Douceur. The *Sybil attack. In First International Workshop on Peer-to-Peer Systems (IPTPS '02),* Mar. 2002.
[3] C. Karlof and D. Wagner. *Secure routing in wireless sensor networks: Attacks and countermeasures*. In First IEEE International Workshop on Sensor Network Protocols and Applications, pages 113–127, May 2003.
[4] J. Newsome, E. Shi, D. Song, and A. Perrig, *The Sybil attack in sensor networks: analysis & defenses*, in Proc. of ACM IPSN, 2004 pp. 259–268.
[5] J. Ledlie and M. Seltzer, *Distributed, secure load balancing with skew, heterogeneity and churn,* in Proc. of IEEE INFOCOM, vol. 2, 2005, pp. 1419–1430.
[6] G. Mathur, V. Padmanabhan, and D. Simon, *Securing routing in open networks using secure traceroute*, in Technical report MSRTR- 2004-66, Microsoft Research, 2004.
[7] P. Bahl and V. Padmanabhan. Radar: *an in-building RF-based user location and tracking system*. In Proceedings of IEEE Infocom, 2000.
[8] 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
[9] 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.
[10] H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao, *SybilLimit: A nearoptimal social network defense against Sybil attack,* IEEE/ACM Trans. Netw., vol. 18, no. 3, pp. 3–17, Jun. 2010.
[11] H. Yu, M. Kaminsky, P.B. Gibbons, and A. Flaxman, *SybilGuard: Defending against Sybil attack via social networks,* IEEE/ACM Trans. Netw., vol. 16, no. 3, pp. 576–589, Jun. 2008.
[12] H. Yu, C. Shi, M. Kaminsky, P. B. Gibbons, and F. Xiao, *DSybil: Optimal Sybil-resistance for recommendation systems*" in Proc.IEEE Symp. Security Privacy, 2009, pp. 283–298.
[13] S. D. Kamvar, M. T. Scholosser, and H. G. Molina, *The Eigen Trust algorithm for reputation management in P2P networks,* in Proc. 12th Int. World Wide Web, May 2003, pp. 640–651.
[14] B.S. Jyothi and D. Janakiram, *SyMon: A practical approach to defend large structured P2P systems against Sybil attack,* Peer-to- Peer Netw. Appl., vol. 4, pp. 289–308, 2011.
[15] B. Yu, C. Z. Xu, and B. Xiao, *Detecting Sybil attacks in VANETs,* J. Parallel Distrib. Comput., vol. 73, no. 3, pp. 746–756, Jun. 2013.
[16] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan. *The Cricket location-support system. In Proceedings of ACM MobiCom*, 2000.

[17] G. Mathur, V. Padmanabhan, and D. Simon, *Securing routing in open networks using secure traceroute, in Technical report* MSRTR-2004-66, Microsoft Research, 2004

[18] N. Sastry, U. Shankar, and D. Wagner. *Secure verification of location claims. In Proceedings of the ACM Workshop on Wireless Security (WiSe 2003)*, September 2003.

[19] F. Musau, G. Wang, and M. B. Abdullahi,Song Guo *Neighbour Similarity Trust against Sybil Attack in P2P E-Commerce,* in Proc. IEEE Transaction on Parallel and FDistributed Systems,Mar. 2015, pp. 824–833.

[20] T. Nguyen, L. Jinyang, S. Lakshminarayanan, and S. M. Chow, *Optimal Sybil-resilient peer admission control*, in Proc. IEEE Int. Conf. Comput. Commun., 2011, pp. 3218–3226.

[21] Rakesh G.V.,S. Rangaswamy, V. hedge, Shoba G., *A Survey of Techniques to Defend Against Sybil Attacks in Sicial Networks*, in Proc. of IJARCCE,May 2014 pp. 6577–6580.

