RESEARCH PAPER | Engineering | Volume - 5 | Issue - 1 | Jan Special Issue - 2015 | ISSN - 2249-555X

A Survey of Sybil Attacks in Wireless Sensor Networks

KEYWORDS

Itesh Sharma	Rajesh Ishwar
PG Student, EC Engineering, SPBPEC,Saffrony, Mehsana	Asst. Professor, EC Engineering, SPBPEC,Saffrony, Mehsana

ABSTRACT The Sybil attack is an attack wherein a reputation system is subverted by a considerable number of forging identities in peer-to-peer networks. By illegitimately infusing false or biased information via the pseudonymous identities, an adversary can mislead a system into making decisions benefiting her. The research on the Sybil defense technique has experienced four phases: (1) traditional security key-based approaches, (2) specific peer-topeer system feature-based solutions, (3) social network-based methods, and (4) social community-based techniques. We present some Sybil defense schemes, including social graph based Sybil detection, behaviour classification based Sybil detection, and mobile Sybil detection with the comprehensive comparisons. Security and performance analysis shows that Sybil attack can be minimized by our proposed neighbor similarity trust.

Introduction

Peer to Peer (P2P) networks range from communication systems like email and instant messaging to collaborative content rating, recommendation, and delivery systems such as YouTube, Gnutela, Facebook, Digg, and Bit- Torrent. They allow any user to join the system easily at the expense of trust, with very little validation control. P2P overlay networks are known for their many desired attributes like openness, anonymity, decentralized nature, self-organization, scalability, and fault tolerance. Each peer plays the dual role of client as well as server, meaning that each has its own control. All the resources utilized in the P2P infrastructure are contributed by the peers themselves unlike traditional methods where a central authority control is used. Peers can collude and do all sorts of malicious activities in the open-access distributed systems. These malicious behaviors 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 behavior 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 [1]. The number of identities that an attacker can generate depends on the attacker's resources such as bandwidth, memory, and computational power [2]. 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. In a P2P e-commerce application scenario, most of the trust considerations depend on the historical factors of the peers. The influence of Sybil identities can be reduced based on the historical behavior and recommendations from other peers. For example, a peer can give positive a recommendation to a peer which is discovered is a Sybil or malicious peer. This can diminish the influence of Sybil identities hence reduce Sybil attack. A peer which has been giving dishonest recommendations will have its trust level reduced. In case it reaches a certain threshold level, the peer can be expelled from the group. Each peer has an identity, which is either honest or Sybil.

We first give the definition of Sybil attacks, and provide the classification of Sybil attacks. Then, we give several realistic systems which are vulnerable to Sybil attacks. After that, defense mechanisms and their corresponding strengths and weaknesses were discussed.

Sensor Network Communication Structure

The sensor nodes are usually scattered in a sensor field as Shown in Fig. Each of these scattered sensor nodes has the capabilities to collect data and route data back to the sink. Data are routed back to the sink by a multichip infrastructure less architecture through the sink as shown in Fig. The sink may communicate with the task manager node via Internet or satellite. The design of the sensor network is as described by Fig. 1. is influenced by many factors, including fault tolerance, scalability, production costs, operating environment, sensor network topology, hardware constraints, transmission media, and power consumption.

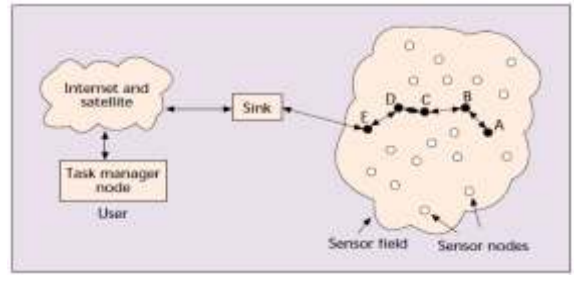

Fig. 1 Structure Sensor Network

Sybil Attack Model

We present a generalized Sybil attack model in Fig. 2, where the serving AP (AP 1) receives service requests from clients, during a specified period of time. A Sybil node attempts to claim identities, in hopes of consuming the AP's resources.

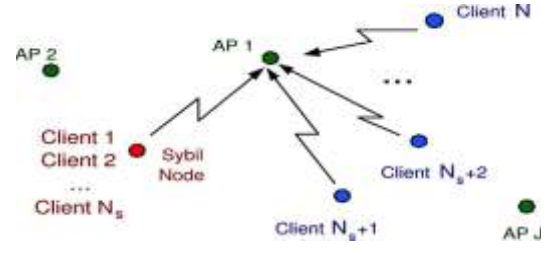

Fig. 2. Sybil attack model with AP 1 receiving messages from clients, where the first clients are actually in the same terminal (i.e., Sybil node), while the remaining clients are legal users in distinct terminals. Sometimes,

Volume - 5 | Issue - 1 | Jan Special Issue - 2015 | ISSN - 2249-555X

more than one (AP cooperates to track channels from these clients.

The remaining clients are legal users at distinct terminals. For convenience of notation, we will refer to the first client's as being from the Sybil node. If the AP does not catch enough Sybil clients, it is likely that some of the legal clients will fail to access network services, especially when is large. The special cases with and , respectively, indicate no Sybil and no legal client. Some wireless networks deploy more than one AP (i.e.,) in the area to improve the quality of service and to increase the number of clients allowed. Without loss of generality, we assume each AP can receive some of the service requests and is able to track the channel from some of the clients.

Radio Resource Testing Result

We present a novel approach to direct validation. As a form of resource testing, this approach relies on the assumption that any physical device has only one radio. We also assume that a radio is incapable of simultaneously sending or receiving on more than one channel as a concrete example, consider that a node wants to verify that none of its neighbors are Sybil identities. It can assign each of its n neighbors a different channel to broadcast some message on

$$\Pr(\text{detection}) = \sum_{\text{all } S,M,G} \Pr(S,M,G)\Pr(\text{detection}|S,M,G)$$

$$= \sum_{\text{all } S,M,G} \frac{\binom{s}{S}\binom{m}{M}\binom{g}{G}}{\binom{n}{c}} \frac{S-(m-M)}{c}$$

Now suppose that we repeat this test for r rounds, choosing a random subset to test and a random channel to listen to in each round. The probability of a Sybil node being detected

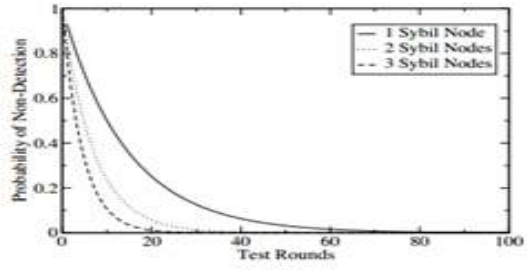

Fig. 3: Probability of no Sybil nodes being detected, using the radio defense, with a channel for every neighbour. Assumes 15 neighbors (including Sybil nodes), any number of which could be malicious.

on which to listen. If the neighbor that was assigned that channel is legitimate, it should hear the message. 2 Suppose that s of the verifier's n neighbors are actually Sybil nodes. In that case, the probability of choosing to listen to a channel that is not being transmitted on, and thus detecting a Sybil node, is n. Conversely, the probability of not detecting a Sybil node is n−s n. If the test is repeated for r rounds, then the chance of no Sybil nodes being detected is (n−s n) r. Figure 3 shows the probability of not detecting the presence of some Sybil nodes using this method. A more difficult case is when there are not enough channels to assign each neighbor a different channel. In this case, a node can only test some subset of its neighbors at one time. If there are c channels, then the node can test c neighbours at once. Note that a malicious node not in the subset being tested can cover for a Sybil node that is being tested by transmitting on the channel that the Sybil node is supposed to be transmitting on. Suppose that in a node's set of n neighbors, there is Sybil nodes, m malicious nodes, and g good (correct) nodes. Of these, a node can only test c neighbors at one time. Of these c neighbors, there are S Sybil nodes, M malicious nodes, and G good (correct) nodes. The probability of a Sybil node being detected is then.

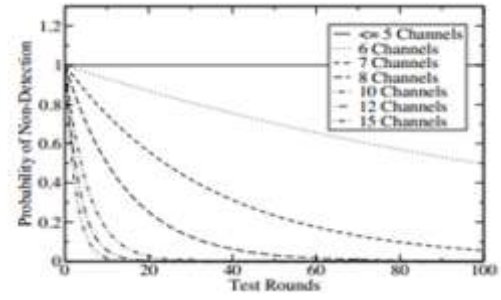

Fig. 4: Probability of no Sybil nodes being detected, using the radio defense, with fewer channels than neighbours. Assumes 5 correct neighbours, 5 malicious and 5 sybil neighbours.

$$\Pr(\text{detection}) = 1 - \Pr(\text{nondetection})^{r_{round}}$$

$$= 1 - (1 - \Pr(\text{detection})_{1round})^{r}$$

Figure 4 shows the probability of an attacker evading detection when using 5 malicious nodes, and generating 5 additional Sybil identities. This is an effective defense against the simultaneous direct-communication variant of the Sybil attack, if the assumptions hold that an attacker cannot use one device to send on multiple channels simultaneously. However, with the advancement of software radio, we will need to adapt this Sybil node detection technique.

Sybil Based Attack

Channel-Based Detection of Sybil Attacks [1]

Due to the broadcast nature of the wireless medium, wireless networks are especially vulnerable to Sybil attacks, where a malicious node illegitimately claims a large number of identities and thus depletes system resources. We propose an enhanced physical-layer authentication scheme to detect Sybil attacks, exploiting the spatial variability of radio channels in environments with rich scattering, as is typical in indoor and urban environments. We build a hypothesis test to detect Sybil clients for both wideband and narrowband wireless systems, such as Wi-Fi and WiMax systems. Based on the existing channel estimation mechanisms, our method can be easily implemented with low overhead, either independently or combined with other physical-layer security methods, e.g., spoofing attack detection. The performance of our Sybil detector is verified, via both a propagation modeling software and field measurements using a vector network analyzer, for typical indoor environments. Our evaluation examines numerous combinations of system parameters, including bandwidth, signal power, number of channel estimates, and number of total clients, number of Sybil clients, and number of access points. For instance, both the false alarm rate and the miss rate of Sybil attacks are usually below 0.01, with three tones, pilot power of 10 mW, and a system bandwidth of 20 MHz.

Sybil Attacks Detection in Vehicular Ad Hoc Networks[2]

Vehicular ad hoc networks (VANETs) are being increasingly advocated for traffic control, accident avoidance, and

Volume - 5 | Issue - 1 | Jan Special Issue - 2015 | ISSN - 2249-555X

management of parking lots and public areas. Security and privacy are two major concerns in VANETs. Unfortunately, in VANETs, most privacy-preserving schemes are vulnerable to Sybil attacks, whereby a malicious user can pretend to be multiple (other) vehicles. In this paper, we present a lightweight and scalable protocol to detect Sybil attacks. In this protocol, a malicious user pretending to be multiple (other) vehicles can be detected in a distributed manner through passive overhearing bys set of fixed nodes called road-side boxes (RSBs). The detection of Sybil attacks in this manner does not require any vehicle in the network to disclose its identity; hence privacy is preserved at all times. Simulation results are presented for a realistic test case to highlight the overhead for a centralized authority such as the DMV, the false alarm rate, and the detection latency. The results also quantify the inherent trade-off between securities, i.e., the detection of Sybil attacks and detection latency, and the privacy provided to the vehicles in the network. From the results, we see our scheme being able to detect Sybil attacks at low overhead and delay, while preserving privacy of vehicles.

Lightweight Sybil Attack Detection in MANETs [3]
Fully self-organized mobile ad hoc networks (MANETs) represent complex distributed systems that may also be part of a huge complex system, such as a complex system-of-systems used for crisis management operations. Due to the complex nature of MANETs and its resource constraint nodes, there has always been a need to develop lightweight security solutions. Since MANETs require a unique, distinct, and persistent identity per node in order for their security protocols to be viable, Sybil attacks pose a serious threat to such networks. A Sybil attacker can either create more than one identity on a single physical device in order to launch a coordinated attack on the network or can switch identities in order to weaken the detection process, thereby promoting lack of accountability in the network. In this research, we propose a lightweight scheme to detect the new identities of Sybil attackers without using centralized trusted third party or any extra hardware, such as directional antennae or a geographical positioning system. Through the help of extensive simulations and real-world test bed experiments, we are able to demonstrate that our proposed scheme detects Sybil identities with good accuracy even in the presence of mobility.

SybilGuard: Defending Against Sybil Attacks via Social Networks [4]
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 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.

Sybil Attacks and Their Defenses in the Internet of Things [5]
The emerging Internet-of-Things (IoT) are vulnerable to Sybil attacks where attackers can manipulate fake identities or abuse pseudo identities to compromise the effectiveness of the IoT and even disseminate spam. In this paper, we survey Sybil attacks and defense schemes in IoT. Specifically, we first define three types Sybil attacks: SA-1, SA-2, and SA-3 according to the Sybil attacker's capabilities. We then present some Sybil defense schemes, including social graph based Sybil detection, behaviour classification based Sybil detection, and mobile Sybil detection with the comprehensive comparisons. Finally, we discuss the challenging research issues and future directions for Sybil defense in IoT.

Channel-Based Detection of Sybil Attacks in Wireless Networks [6]
Due to the broadcast nature of the wireless medium, wireless networks are especially vulnerable to Sybil attacks, where a malicious node illegitimately claims a large number of identities and thus depletes system resources. We propose an enhanced physical-layer authentication scheme to detect Sybil attacks, exploiting the spatial variability of radio channels in environments with rich scattering, as is typical in indoor and urban environments. We build a hypothesis test to detect Sybil clients for both wideband and narrowband wireless systems, such as Wi-Fi and Wi-Max systems. Based on the existing channel estimation mechanisms, our method can be easily implemented with low overhead, either independently or combined with other physical-layer security methods, e.g., spoofing attack detection. The performance of our Sybil detector is verified, via both propagation modelling software and field measurements using a vector network analyzer, for typical indoor environments. Our evaluation examines numerous combinations of system parameters, including bandwidth, signal power, number of channel estimates, and number of total clients, number of Sybil clients, and number of access points. For instance, both the false alarm rate and the miss rate of Sybil attacks are usually below 0.01, with three tones, pilot power of 10 mW, and a system bandwidth of 20 MHz.

CONCLUSION
Peer-to-peer systems play an ever-increasingly important part of our daily lives. However, most of the peer-to-peer systems are vulnerable to Sybil attacks. In order to design more efficient and practical Sybil defences, we write this survey. This article is the first survey focusing on the developments of Sybil defenses. Unlike other surveys, we describe these mechanisms according to anti-Sybil approaches' developing stages. By the end of this survey, we provide some directions for future research.

REFERENCE
[1] Liang Xiao, Larry J. Greenstein, Narayan B. Mandayam, Wade Trappe. "Channel-Based Detection of Sybil Attacks in Wireless Networks" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 4, NO. 3, SEPTEMBER 2009. | [2] Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty "P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 3, MARCH 2011. | [3] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat "Lightweight Sybil Attack Detection in MANETs" IEEE SYSTEMS JOURNAL, VOL. 7, NO. 2, JUNE 2013. | [4] Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, Member, IEEE, and Abraham D. Flaxman "SybilGuard: Defending Against Sybil Attacks viaSocial Networks" IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 16, NO. 3, JUNE 2008. | [5] Liang Xiao, Student Member, IEEE, Larry J. Greenstein, Life Fellow, IEEE, Narayan B. Mandayam, Fellow, IEEE,and Wade Trappe, Member, IEEE "Channel-Based Detection of Sybil Attacksin Wireless Networks" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 4, NO. 3, SEPTEMBER 2009. | [6] Kuan Zhang, Student Member, IEEE Xiaohui Liang, Member, IEEE Rongxing Lu Member, IEEE and Xuemin (Sherman) Shen Fellow, IEEE. Sybil Attacks and Their Defenses in the Internet of Things DOI 10.1109/JIOT.2014.2344013, IEEE Internet of Things Journal.