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

Survey on RSSI Based Sybil Defense

Akshaya.S.U[1], Dr. Thilagavathi.D[2]

P.G Scholar, Department of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, India[1]

Professor and Head, Dept. of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, India[2]

Abstract: Wireless network is a self-organized and distributed controlled network. The ad-hoc network is a decentralized wireless network because it does not depend on a pre-existing infrastructure or wireless network. Sybil attack which is commonly called as Pseudo-spoofing in early 2002. The attack is harmful against wireless ad hoc network, in which the node claims multiple identities to gain unfair influences. The Sybil countermeasures deals with various methodology to Prevention, detection, Recovery of Sybil nodes. RSSI is detection technique which is used in IEEE 802.11 standards without using any trusted sources. RSSI observation is made practical in commodity devices to defense against Sybil attackers in network without any trust devices. The survey on 10 studies is concentrated in this area published during 2005-2014. We summarize our observation with common pitfall among the survey work.

Key words: Sybil attack, RSSI, IEEE 802.11, Trusted Sources.

I. INTRODUCTION

Wireless ad-hoc network are decentralized type of network, it does not rely on a pre-existing infrastructure. Mobile ad-hoc network are a kind of wireless ad-hoc network in which nodes are free to move. MANET has many challenges [1] like power awareness, dynamic topology, multicast routing, security and quality of services. Security is extremely important scenario because the wireless ad-hoc network becoming vulnerable due to Sybil attack, the attacker subverts the reputation system by creating number of pseudonymous identities in order to gain disproportionately larger influences.

There are many defense against Sybil attack based on Sybil attack countermeasures [2]. The counter measures (Figure 1) are categorized into Sybil attack: Prevention, detection, Recovery. Proposed prevention techniques based on the trusted certification, which uses the certification authority which is not practical in open wireless network.

However there are Sybil recovery which actually does not perform recover mechanism, i.e. by Sybil recovery the malicious nodes are not been removed from the network instead it performs techniques namely self-healing, isolation, logical removal. In which data transmission is denied from those malicious nodes.The survey observed that Sybil detection has finite counter measures to defense against Sybil attack. The various techniques such as recurring cost, incentive based technique, resource testing, social networks based techniques, misbehavior detection, and localization method. Accordingly the survey is focused on the technique that makes Sybil defense to be practical for wireless ad-hoc network of commodity 802.11 devices. The localization method under Sybil defense, i.e. RSSI, uses the spatial correlation between the signal strength and physical location of a node to find out the presence of the Sybil node. RSSI found to be the defense exposed on commodity 802.11 devices where it does not required any hardware equipment to be implemented in defense against Sybil attack in open wireless ad-hoc network which does not allow any trusted sources (e.g., corporate access point) to monitor the performance of network.

In this paper, we focus on research in the area of Sybil detection, specifically, the work published during the period of 2002-2015. We analyze major components in each study for the evaluation and comparison of the Sybil detection techniques. These components include the characteristics of the performed experiments and the methods used for performance evaluation. The paper is organized as follows: Section II presents the overview of the related work. In Section III, we present our evaluation methodology. Finally, Section IV concludes the survey and provides some future directions.

II. RELATED WORK

In the literature, the problem of Sybil attack has be survived widely in the context wireless network, ad hoc network, mobile ad hoc network, etc. with some significant reported works related to this problem identification are as follows. The overview classification of paper is presented in Table 1.

Hongbo Zhou, (2005) has proposed scheme named Multiple–key Cryptography-based Distributed certification Authority [3]. In the scheme, every server node is required to generate signature. As long as there is a good server node, including malicious node has many identities it cannot forge signature of DCA. Compared to the threshold scheme, MC-DCA scheme is vulnerable to Sybil attack achieve lower communication overhead, moderate latency. The inference of from this paper is usage of certification authority which is not practically for commodity 802.11 device.

Daniel B. Faria, (2006) used a signal print [4] technique to defense against the sybil attack. The transmitting devices can be robustly identified by its signal print, a tuple of signal strength values reported by access point which acting as sensors.

DOI 10.17148/IJARCCE.2015.4908

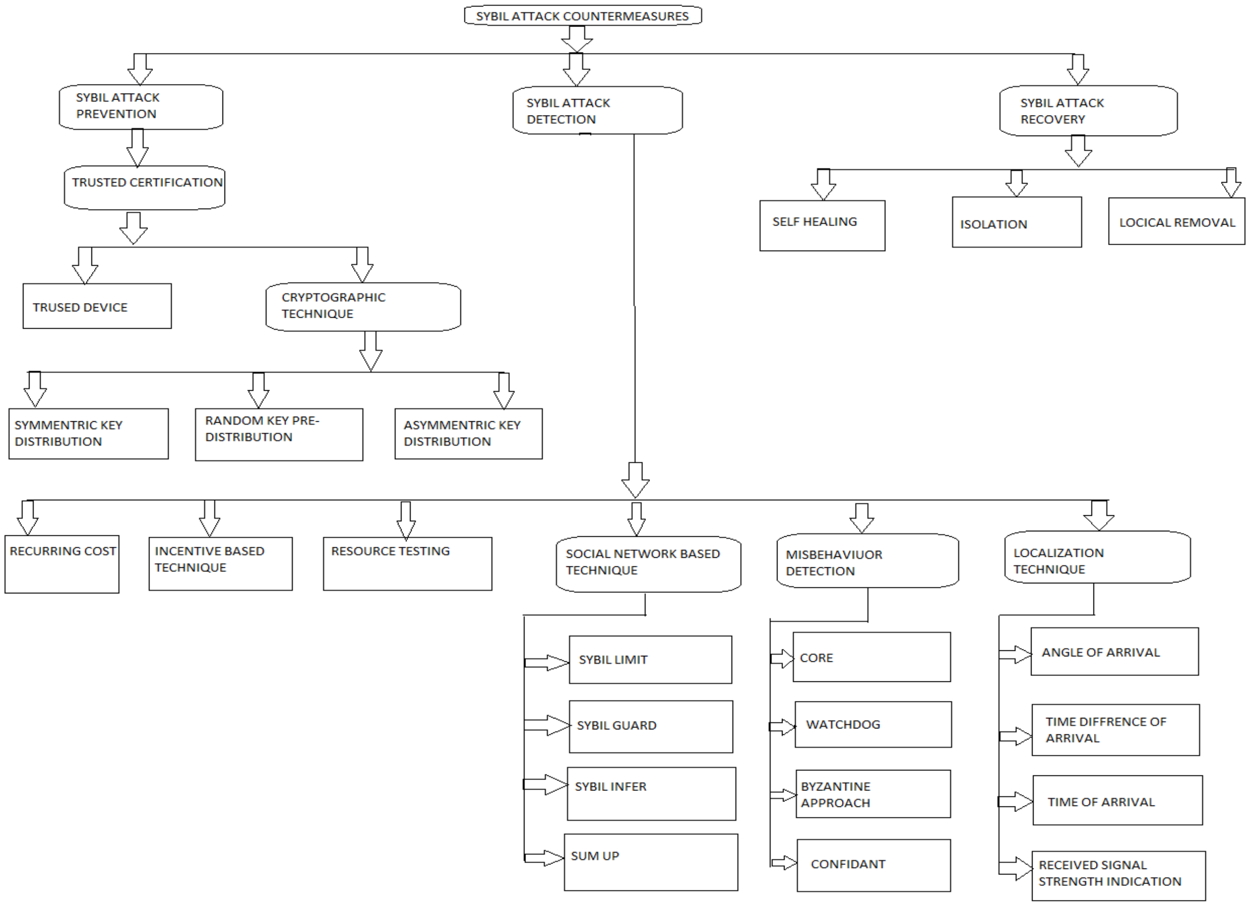

Figure 1: Sybil attack Counter Measures

The signal print is reliable client idetifiers which creates signal strength measurement. The malicious clients can lie about their MAC address, signal print are strongly correlated with the physical location. Therefore, holding packets with their signal prints provides the crafting of proper matching rules. Signal print has the advantage that wireless network is able to detect a large class of effective DOS based on MAC address spoofing. The inference of from this paper is usage of access point which is not ablicable in open wireless network.

Liang Xiao, (2009) proposed a channel based authentication technique [5]. The proposed technique enhanced physical layer authentication scheme to detect Sybil attack to overcome the drawback of existing technique named channel estimation mechanism. First, the channel based authentication technique exploits the spatial variability of radio channels in environment with rich scattering, i.e. typical in indoor and urban environment.

Second, build a hypothesis test to detect Sybil clients for both wideband and narrowband wireless systems, such as Wi-Fi and Wi-MAX system. The test statistics that is chosen based on: the number of claimed identities, the number of access point. The limitation associated with channel path loss thus performance degrades in this case. Implementing multiple access points can overcome this limitation. The drawback of Access points is the inference in this paper.

Diogo Monica, (2009) defines a framework to evaluate the power and performance of radio resource test (RRT) [6], i.e. A technique that allows the detection of Sybil identities. RRT assumes each node has access to a single radio devices, the potential to support protocol that do-not require pre-configuring nor pre-shared secrets. The proposed take the advantage of improving the scalability of the networks but get holds of large amount of network resources to complete malicious task.

Yingying Chen, (2010) observed the identity of a node can be verified through cryptographic authentication, authentication is not always possible because it required key management and additional infrastructure. Therefore, proposed a generalized attack-detection model that utilizes the spatial correlation of received signal strength (RSS) [7]. RSS includes K-means algorithm, it is used to derive the test statistics for detection of identities-based attacks. RSS advantage is take as the inference for the Sybil defense in IEEE 802.11 devices.

Abedelaziz Mohaisen, (2011) proposed a novel algorithm called Biasing random walk [8]. The observed relationship between the qualities of the algorithm property which proposes a several designs, each in form of modified random walk to model trust in social network. Further learn the impact of different design on the performance of the Sybil defenses by comparing them to each other when operated on Sybil-Limits, i.e. a design for

DOI 10.17148/IJARCCE.2015.4908

defensing against the Sybil attack using social network. It is applicable only in monotonic polices, i.e. it works only in transmission power where either never decrease or never increase.

Yue Liu, (2013) proposed a method Multiple-input Multiple-Output (MIMO) [9] in Sybil defense followed by resource testing. In MIMO the received signal is examined to identify the transmission. The node is identified to be a Sybil or malicious node when it is receives multiple identities from same receiver. MIMO gains complete information about the received signal. Usage of resource testing can be easily defeated in the ad-hoc network of resource limited mobile devices is addressed as the inference.

Winnarasi. A, (2013) introduced a lightweight scheme to detect the identities of Sybil attackers. RSS (Received Signal Strength) [10] is a value to find the lightweight of the node in MANET. It is used to differentiate the legimate nodes and Sybil identities. RSS does not require any utilization technique and any directional antenna or any GPS equipment. It requires any data security algorithm to be combined with RSS scheme, which can be used to detect Sybil attack and provide secure communication which makes efficient security scheme with any protocol.

Danish Shehzad, (2014) proposed a novel mechanism [11] that ensures the detection of both simultaneous Sybil node in the network and Join and Leave Sybil attack in the network. Two mechanism are handled: First, Hash Function mechanism. Second, Request threshold validation for detection of join and leave Sybil. Since the both the mechanism does not compromise it identities in the network the false positive rate is high.

TABLE 1

Year	**Title**	**Method for Sybil Defense**	**Counter Measures**
2005	Multiple-key Cryptography-based Distributed Certificate Authority in Mobile Ad-hoc Networks	Multiple-key Cryptography-based Distributed Certificate Authority	Trusted certification
2006	Detecting Identity -Based Attacks in Wireless Networks Using Signal-Prints.	Signal Print	Localization Method
2009	Channel-Based Detection of Sybil Attacks in Wireless Networks	Channel – based Authentication technique	Trusted certification
2009	On the Use of Radio Resource Tests in Wireless ad hoc Networks.	Radio Resource Test	Localization Method
2010	Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks	Received Signal Strength(RSS)	Localization Method
2011	Keep your friends close: Incorporating trust into social network-based Sybil defences.	Biasing random walks	Social Network-based
2013	Extending Channel Comparison Based Sybil Detection to MIMO Systems.	MIMO (Multiple-input Multiple-Output)	Resource Testing
2013	Lightweight Scheme to Detect the New Identities of Sybil Attackers in MANETS.	Received Signal Strength	Localization Method
2014	A Novel Mechanism for Detection of Sybil Attack in MANETs	Novel Mechanism	Localization Method
2014	A Moving Target Defense Mechanism for MANETs Based on Identity Virtualization	MTD mechanism	Localization Method

DOI 10.17148/IJARCCE.2015.4908

Massimiliano Albanese, (2014) proposed a defense mechanism [12] for protecting the identities of node in MANET and defeat the attacker by reconnaissance effort. The proposed mechanism brings the Sybil into a effective defense mechanism. Here the network layer is modified by introducing the translation services for mapping virtual identities and a protocol for propagation updates of a node's virtual identities to all disappropriate node. Whereas, by updating protocol update frequency can be controlled by tuning. The inference is defense against the moving node consumes high energy.

III. EVALUATION METRICS

I. RSSI based Sybil defense

RSSI (Received Signal Strength Indication) [13] can be validated by Transmitter ID's. For example, by receiving the message the receiver can associate with RSSI of the message with sender ID, later some other message with same RSSI but from different sender ID, the receiver can identify that the message is from Sybil attacker. Hence by using ratio of RSSI from multiple nodes we can implement the Sybil defense technique.

II. RSSI based localization

Localization technique is a process of find out the global position to calculate a node's position with respect to other nodes.

(1) RSSI at i for a transmission from node 0 with power P0

$$R_{i=}\,P_0K/d_i^{\propto} \qquad \text{---- (1)}$$

(2) RSSI ratio of node i to node j

$$\frac{R_i}{R_j} = \left(\frac{P_0.K}{d_i^{\propto}}\right)\Big/\left(\frac{P_0\ .K}{d_j^{\propto}}\right) = \left(\frac{d_j}{d_j}\right)^{\propto} \text{---- (2)}$$

By cancelling P0 value in ratio of RSSI, this not affected by change in transmission power.

(3) Since it is a localization technique the location (x,y) of node can be calculated by knowing i , j, k, l.

$$\begin{aligned}(x-x_i)^2+(y-y_i)^2 \quad &= \left(\frac{R_i}{R_j}\right)^{\frac{1}{a}}((x-x_i)^2+(y-y_i)^2)\\ &= \left(\frac{R_i}{R_k}\right)^{\frac{1}{a}}((x-x_k)^2+(y-y_k)^2)\\ &= \left(\frac{R_i}{R_l}\right)^{\frac{1}{a}}((x-x_l)^2+(y-y_l)^2) \text{ --- (3)}\end{aligned}$$

III. RSSI based detection

The Sybil attack can be detected by comparing the ratio of RSSI for received message. The message can be computed by calculating D$_i$.

$$\frac{R_{Di}^{Si}}{R_{Di+1}^{Si}} \quad \text{--- (4)}$$

Di - Detects a Sybil attack.
Si - Sybil node tries to forge ids.
Computing Di,

$$\frac{R_{Di}^{Si}}{R_{Di+1}^{Si}} < \sigma \quad \text{--- (5)}$$

IV. CONCLUSION

MANET holds a devices which is free to move independently in any direction in which continuously self-configuring, infrastructure-less network. MANET has become popular due to growth of laptop and 802.11/Wi-Fi wireless networking. Sybil attack is an active attack which takes place in network layer. The prevention, detection and recovery mechanism against the Sybil attack is performed. Among the counter measures RSSI is found to be practically applicable for 802.11 standards, i.e. the standard does not allow any physical devices to monitor their actives in networks. Thus the survey classified RSSI from other countermeasures in defense against Sybil node.

REFERENCES

[1] Suraj Thawani, Hardik Upadhyay, "A Survey on Securing TORA for Detecting and Protecting Against Sybil Attack in MANETs", e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com Volume 10, Issue 11 (November 2014), PP.64-69

[2] Aditi Paul, Somnath Sinha, and Sarit Pal, "An Efficient Method to Detect Sybil Attack using Trust based Model", Proc. of Int. Conf. on Advances in Computer Science, AETACS

[3] Hongbo Zhou, Matt W. Mutka, Lionel M. Ni, "Multiple-key Cryptography-based Distributed Certificate Authority in Mobile Ad-hoc Networks". 0-7803-9415-1/05/$20.00 (C) 2005 IEEE.

[4] Daniel B. Faria, David R. Cheriton, "Detecting Identity -Based Attacks in Wireless Networks Using Signalprints", WiSe'06, September29, 2006, LosAngeles, Calfornia, USA. Copyright 2006 ACM1-59593 557-6/06/0009...$5.00.

[5] 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.

[6] D. Monica, J. Leitao, L. Rodrigues, and C. Ribeiro, "On the use of radio resource tests in wireless ad hoc networks," in Proc.3rd WRAITS, 2009.

[7] Yingying Chen, Jie Yang, Wade Trappe, and Richard P. Martin, "Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 59, NO. 5, JUNE 2010.

[8] Abedelaziz Mohaisen, Nicholas Hopper, and Yongdae Kim, "Keep your friends close: Incorporating trust into social network-based Sybil defenses", INFOCOM, 2011 Proceedings IEEE , 10.1109 / INFCOM. 2011. 5934998.

[9] Y. Liu, D. R. Bild, R. P. Dick, "Extending channel comparison based Sybil detection to MIMO systems," Tech. Rep. CSE-TR-584-13, Dept. of Electrical Engineering and Computer Science, University of Michigan, Nov. 2013.

[10] Winnarasi. A, Sasikala.V, "Lightweight Scheme to Detect the New Identities of Sybil Attackers in MANETS", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 3 Issue 3, March – 2014.

[11] Danish Shehzad, Dr. Arif Iqbal Umar, Noor Ul Amin, and WaqarIshaq, "A Novel Mechanism for Detection of Sybil Attack in MANETs", International conference on Computer Science and Information Systems (ICSIS'2014) Oct 17-18, 2014 Dubai (UAE).

[12] Massimiliano Albanese, Alessandra De Benedictisy, Sushil Jajodia, and Kun Sun, "A Moving Target Defense Mechanism for MANETs Based on Identity Virtualization". In the First IEEE Conference on Communications and Network Security (CNS), Washington D.C., USA, October 14-16, 2013.

[13] Murat Demirbas, Youngwhan Song, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks" IEEE Computer Society Washington, DC, USA ©2006, ISBN: 0-7695-2593-8.

DOI 10.17148/IJARCCE.2015.4908