International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.6., 2015
(Nov.-Dec.,)

RESEARCH ARTICLE

ISSN: 2321-7758

IDENTIFYING OF SYBIL ATTACK USING RECEIVED SIGNAL STRENGTH (RSS) IN MANETS- A SURVEY

MUJAMIL DAKHANI[1], MOHAMMAD TAYAB DAFFEDAR[2]

[1,2]Department of Computer Science and Engineering,
Secab Institute of Engineering & Technology, Vijayapur, Karnataka, India
Nauraspur, Bagalkot road, vijayapur, Karnataka, India

MUJAMIL DAKHANI

ABSTRACT

Manets are susceptible to various kinds of attacks such as Sybil Manets attacks. In this work, we focus to present practical estimation of capable method for detecting lightweight Sybil Attack. Sybil attack is an attack where malicious user form many fake identities and entrance the system from many various modes. In Sybil attack, network attackers divert the accuracy count by incrementing its trust and decrementing others. This type of attacks lead into main information loss and hence misunderstanding in the network, but it also decreases the trustworthiness surrounded by different mobile nodes. In this work, the aim of these is to detect the lightweight Sybil attack with aim of finding the new identities of Sybil attacker without using any different resource such as hardware or any trusted third party (TTP). In this paper work, The Approach explores is depend on use of Received signal strength (RSS) to detect Sybil attacker. This approach uses the RSS in order to compare between the legitimate and Sybil identities.

Keywords—MANETS, and RSS: Received Signal Strength, Sybil Attack, Threshold, and UB: Upper bound

I. Introduction

As we are well-known to Mobile Ad hoc network (MANET) which is usually consisting of mobile, radio device over the wireless communication channel. This type of network does not want any settled infrastructure and data communication or routing is done as when we want. This type of network is susceptible to various kinds of security attacks such as Sybil attacks, black hole attacks, and wormhole attacks.

MANET Characteristics**:**

- Dynamically changing network topology
- Lack of centralized monitoring
- Cooperative algorithms
- Bandwidth constraint
- Limited physical security
- Energy constrained operation

The paper is planned as follows. Section 2 provides an overview of Sybil attack, and some of the Sybil attacks Detection Techniques, section 3 deals with some related work to detect the Sybil attack, section 4 presents a various methodologies to identify Sybil attacks and finally conclude the paper in Section 5.

II. Overview of Sybil Attack

Sybil attack is an attack which uses several identities at a time and increases lot of misjudgements among the nodes of a network or it may use identity of other legitimate nodes present in the network and creates false expression of that node in the network. To have secure communication it is necessary to eliminate the Sybil nodes from the network

The following goals must be fulfilled by security algorithm used to detect the attack:

1. Authentication: It means that each and every node, participating in communication must be genuine and legitimate node.
2. Availability: All services should be available all the time to all the nodes for the proper functioning and security of the network.
3. Integrity: It gives the assurance that the data received by the receiver will be same as the data send by the sender.
4. Confidentiality: It means that some data is only accessible by the authorized users.
5. Non-repudiation: It means sender and receiver cannot deny that they didn't send or receive the data.

In Manets, Sybil attacker destroy Mobile Ad hoc network in various ways. Such kind of attacks will causes on basic functionalities of wireless network. Therefore once needs to have power full secure method which not only find such attacker in Mobile ad hoc network but also make less severe them from motivating serious loss in networks. The lastly used method for checking the Sybil attacks depends on the use of cryptographic or trusted certification based authentication. But the restriction of the approach is that it wants costly start up setup and also leads into more overhead in order to supporting as well as distributing cryptographic keys. Some other methods are based on the use of received signal strength for finding the Sybil attackers in mobile ad hoc networks.

Mobile ad hoc networks (MANETs) have concerned a set of kindness due to their attractive and capable functionalities including mobile safety, traffic congestion avoidance, and location based services. Privacy is a main problem in MANETs. As the wireless communication channel is a shared medium, exchanging messages without any security protection over the air can easily leak the information that users may want to keep private. As the wireless communication channel is a shared medium, exchanging messages without any security protection over the air can easily leak the information that users may need to keep the information private. Pseudonym based schemes have been introduced to preserve the location privacy of mobile. However, those schemes needs the mobile to store a huge number of pseudonyms and certifications, and do not support some important secure functionality such as authentication and integrity. This approach uses RSS for comparing identities of Sybil node and lawful node.

The centralized key management has some disadvantages. The system maintenance is not flexible. Another problem regarding the centralized key management is that many existing schemes assume a tamper-proof device being installed in each node. The tamper-proof device costs several thousand dollars. The framework to be developed in this work does not require the expensive tamper-proof device**.** Here in this technique inside the network each and every node will learn or keep trace on the overall history of all other nodes dynamically to know about it, So when there will be the small change in any of the nodes behaviour then other nodes would come to know that node is misbehaving or is a attacker node eventually this will be done using nodes entry and exit behaviour itself, this technique requires no costly hardware resources. And Sybil Attack Detection Techniques are as follows shown in table I

TABLE I: SYBIL ATTACK DETECTION TECHNIQUES

SL no.	Mechanism Name	Architecture	Summary
1	Lightweight Sybil Attack Detection	Distributive	The nodes entering in the network with speed greater than the threshold speed are detected as Sybil nodes

2	Robust Sybil Attack Detection	Distributive	The nodes having the same path or pattern are detected as Sybil nodes
3	Secure Address Allocation	Distributive	The Sybil attack is prevented as Unique addresses are allocated to Each node in the network.
4	Received Signal Strength Based	Distributive	Plot the RSS of nodes in order to determine and visualize the behaviour of the new legitimate nodes and the Sybil attackers

III. RELATED WORK

In [1], Sohail Abbas, Madjid Merabti, introduce a lightweight scheme to detect the new identities of Sybil attackers without using centralized trusted third party or any extra hardware like directional antennae or a geographical positioning system (GPS). With the help of simulation and real word experiments, able to pointing out that our introduced scheme detects Sybil identities with good accuracy even in the presence of mobility.

In [2], J.Newsome, E.Shi, D. Song, and A.Perrig, analyses the threat posed by the Sybil attack to wireless sensor networks. In this here pointing out that the attack can be increasing damages to multiple important functions of wireless sensor network like routing, resource allocation, and misbehavior detection. Then introduce different novel techniques to defend against the Sybil attack, and analyse their effectiveness quantitatively.

In [3], S. Hashmi and J. Brooke, presents an authentication mechanism for MANETs that utilizes hardware id of the device of each node for authentication. An authentication agent is developed that verifies the hardware id of the authenticate node. A comprehensive defense model is employed to protect the authentication agent from different multiple static and dynamic attacks from a potentially malicious authenticate node. Security of authenticate node is assured by involving a TTP that signs the authentication agent, verifying that it will perform only intended function and is safe to execute.

In [4], Y. Chen, J. Yang, and R. P. Martin, introduce a approach for detecting both spoofing and Sybil attacks by using some set of techniques. First introduce a generalized attack-detection model that utilizes the spatial correlation of received signal strength (RSS) inherited from wireless nodes. Further we supply a theoretical analysis of our method then drawn from the test statistics for detection of identity-based attacks by using the *K*-means algorithm.

In [5], Danish Shehzad el at. Proposed a detection technique based on Hash Function, only messages along with their hash function are accepted each individual node detects Sybil attackers by validating the Hash received along with message by neighbor, after receiving message node gets Hash of sender and compares it with the previous Hash received in Hello message for the validation of its identity. If Identity or Hash differs to that of Hash received along with hello message than node is nominated as Sybil and node is blocked from any communication.

In [6], Levine et al. presented the review of counter measures against Sybil attacks and categorized these techniques as follows.

In [7], Sybil attack was first introduced by Douceur. According to Douceur there is no practical solution for this attack. Deploying Trusted Certification is the only scheme that can completely eliminate the Sybil attack. However, it suffers from costly initial setup, lack of scalability and a single point of attack or failure. Also, it's based on the assumption that each entity has single identity which is very difficult to achieve on the large network. Trusted Certification solution is presented. It is considered to be one of a good preventive solution for Sybil attacks in which a centralized authority is employed for establishing a Sybil-free domain of identities. Each entity in the network is bound to a single identity certificate. But trusted certification suffers from costly initial setup, lack of scalability and a single point of attack or failure.

In [8], resource testing based method presented in which various tasks are distributed to all identities of the network in order to test the resources of each node and to determine whether each independent node has sufficient resources to accomplish these tasks. These tests are carried out to check the computational ability, storage ability and network bandwidth of a node. A Sybil attack will not possess a sufficient amount of resources to perform the additional tests imposed on each Sybil identity. Limitation of this method is that an attacker can get enough hardware resources, such as storage, memory, and network cards to accomplish these tasks.

Piro et al. [9] proposed a detection technique for detection of Sybil nodes by examining the behaviour of nodes. According to the Piro, nodes which move freely, independently in different directions are considered as legitimate nodes and the nodes which moves together are considered as Sybil nodes and it keeps observing these suspected nodes

In [10], P.Kavitha, C.Keerthana, V.Niroja, Vivekanandhan proposed to use passive ad hoc identity technique and key distribution. Detection can be done by a single node, or multiple trusted nodes can join to improve the accurateness of detection. The proposed NDD algorithm-based detection mechanism to Sybil attacks. Use these algorithms to transfer the data in source to destination without any harm or loss as well as each node to have the neighbour's node address. Being subject to on the address the data will be transmitted in to correct endpoint.

IV. VARIOUS METHODOLOGIES TO IDENTIFY SYBIL ATTACK

The various methodologies to identify Sybil attacks projected by some authors are analysed Based on some important constraint and drawbacks illustrated in Table II.

TABLE III: VARIOUS METHODOLOGIES TO IDENTIFY SYBIL ATTACK

Author	Title	Methodology	Drawback
SohailmAbbas Madjid Merabti, and Kashif Kifayat	Lightweight Sybil Attack Detection in MANETs	Received Signal Strength (Rss) Based	Verification accuracy is Limited
J.Newsome E.Shi, D. Song, and A.Perrig	The Sybil attack in sensor networks	Random key distribution And Trusted certification	Leads into more overhead
S.Hashmi and J. Brooke	Toward Sybil resistant authentication in mobile ad hoc networks	Authentication Mechanisms	
Y. Chen, J. Yang, and R. P. Martin	Detecting and localizing identity-based attacks in wireless and sensor networks	generalized attack-detection model and K-means algorithm.	
Danish Shehzad	A Novel Mechanism for Detection of Sybil Attack in MANETs	Hash Function	

Levine et al	A survey of solutions to the Sybil attack	Trusted certification, Resource testing	A single point of attack or failure
J. R. Douceur	The Sybil attack	Trusted certification	Initial setup costly , lack of scalability
D. Monica, J. Leitao, L. Rodriguez, and C. Ribeiro	On the use of radio resource tests in wireless ad hoc networks	Resource testing	Attacker can get enough hardware resources, such as storage, memory
C. Piro, C. Shields, and B. N. Levine	Detecting the Sybil attack in mobile ad hoc networks	Passive Ad hoc Sybil Identity Detection (PASID)	The accuracy rate declines as each node has fewer chances to hear its neighbour
P.Kavitha, C.Keerthana, V.Niroja, V.Vivekanandhan,	Mobile-id Based Sybil Attack detection on the Mobile ADHOC Network	passive ad hoc identity method and key distribution	packet loss Overhead

V. Conclusions

There are a variety of attacks that hinge on the issue of identity. A survey work carried out to analyzing or solving the Sybil attack, in which one entity appears as many different identities. A number of existing methodologies and respective algorithms are proposed for detection of Sybil attack in MANETS. This paper lists out various works accomplished to identify and mitigating Sybil attack in MANET. There is no fixed reliable procedure to detect attack because of costly initial setup and lack of scalability.

References

[1]. 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.

[2]. J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defences," presented at the 3rd Int. Symp. Information Processing in Sensor Networks (IPSN), 2004, pp. 259–268

[3]. S. Hashmi and J. Brooke, "Toward Sybil resistant authentication in mobile ad hoc networks," in Proc. 4th Int. Conf. Emerging Security Inform., Syst. Technol., 2010, pp. 17–24.

[4]. Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," IEEE Trans. Veh. Technol., vol. 59, no. 5, pp. 2418–2434, Jun. 2010.

[5]. 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 (UA).

[6]. B. N. Levine, C. Shields, and N. B. Margolin, "A survey of solutions to the Sybil attack"

[7]. J. R. Douceur, “The Sybil attack,” presented at the Revised Papers from the First Int. Workshop on Peer-to-Peer Systems, 2002, pp. 251–260.

[8]. 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, pp. 21–26.

[9]. C. Piro, C. Shields, and B. N. Levine, “Detecting the Sybil attack in mobile ad hoc networks,” in Proc. Securecomm Workshops, 2006, pp. 1–11

[10]. P.Kavitha, C.Keerthana, V.Niroja, V.Vivekanandhan, “Mobile-id Based Sybil Attack detection on the Mobile ADHOC Network” International Journal of Communication and Computer technologies Volume 02 – No.02 Issue: 02 March 2014 ISSN NUMBER: 2278-9723