ICEST-2K24 [International Conference on Engineering, Science and Technology]
In Association with
International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN - 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

Sybil Attack Detection in Lightweight Sybil Attack in Moving WNS

Suchita M. Yadav[1], Dr. Prasadu Peddi[2], Dr.Satish R Todmal[3]
[1]Research Scholar, Shri.JJT University, Churella, Jhunjhunu, Rajasthan, India
[2]Professor and Ph.D Guide, Shri.JJT University, Churella, Jhunjhunu, Rajasthan, India
[3]Dean Academics, Ph.D, JSPM Imperial College of Engineering & Research, Wagholi, Pune, Maharashtra, India

ABSTRACT
No specialist equipment or antennas are required for this approach to operate. With its assistance, Sybil Attacks could be discovered. This process consists of the following three steps: Sybil node types include: Two types of Sybil nodes exist. In order to deceive or avoid detection, it creates and uses many identities at once in the initial instance. In the second type, it is limited to assuming a single identity at once. Value threshold: Ordinary nodes move at a maximum speed of 10 m/s, which is the foundation for the following phase. Any node faster than 10 m/s is considered a Sybil node. This comparison stage determines the upper maximum threshold value for lightweight. The lightweight values of nodes are averaged at a speed of 10 m/s to determine the highest limit.

I. INTRODUCTION

In crisis management, for example, a complex system-of-systems may include sophisticated dispersed systems like completely Ad hoc mobile networks that self-organize. Due to the intricate architecture and constrained resources at each node, lightweight security solutions have long been necessary. For security mechanisms to operate correctly, each node need its own permanent identity, making Sybil assaults all the more important. Sybil attackers may encourage a lack of accountability in the network by, for example, launching a coordinated assault using several identities generated on a single physical device or by attempting to degrade detection by swapping identities. Here, we provide a lightweight approach that, devoid of specialized hardware or a central trusted third party, has the ability to identify the changing identities of Sybil attackers. We show that our proposed system can accurately discover Sybil identities despite the existence of mobility via comprehensive simulations and experimentation on a real-world test bed. Two types of Sybil nodes should be considered separately. In the first, it takes on several personas simultaneously, either by mimicking others or by making up whole new ones. When using Type 2, only one identity is used at a time.

1. At this stage, we set a threshold value of 10m/s, assuming that average network nodes travel at a slower pace. Sybil nodes are defined as those with velocities higher than 10 m/s.

2. In this comparison stage, the maximum threshold value for RSS (Received Signal Strength) is determined. The RSS value is averaged to find the highest value that may be used for nodes moving at 10 m/s. After accounting for each node, the network's RSS is compared to a maximum value.The inclusion of every node, the RSS of the network is compared to a maximum value. Sybil nodes are those with values that are more than or equal to the maximum RSS value.

The Lightweight Sybil AttackDetection

Technique operates without the usage of any additional hardware or antennas. It is used to identify Sybil assaults. This technique includes the following three steps: Sybil node types: There are two kinds of Sybil nodes. In the first kind, it assumes several identities at once, either by impersonating others' identities or creating its own. Only one identification is used at a time in the second kind. Boundary value: This stage makes the assumption that typical nodes cannot move faster than 10 m/s. Sybil nodes are referred to be nodes with a speed more than 10 m/s.

Identifying Sybil nodes is its purpose. Implementing it does not need any additional hardware or antennas. Therefore, it's inexpensive.

1. **Distinct Characters of Sybil Attack**:

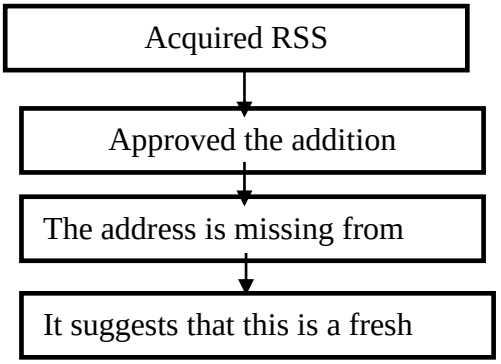
Simultaneous Sybil Attack and Join and Leave, commonly known as Whitewashing Sybil Attack, are two of its characters. One identity is used at a time during a Whitewashing or Join and Leave Attack, and the other identities are forgotten.. Its primary objective here is to undo all of the harm it has done in the past. Furthermore, it makes people less trusting of the network. All of its guises are used simultaneously in Simultaneous Sybil Attack. Its primary goal is to gather more information about the network while simultaneously using more resources, which will cause congestion and confusion.

2. **Enquiry Based on Signal Strength:**

Next, every node in the network will gather data on the RSS values of its nearby peers. Nodes may be classified as authentic or Sybil based on their RSS value. To be deemed a valid node, a newly joined node must have a low RSS value; otherwise, it is called a Sybil node. To keep track of information about its neighbours, each node uses the format.

Exposure of Sybil Nodes:

As a minimum allowable speed, we assume that no legitimate node may go faster than 10 m/s, which is also referred to as the threshold speed. An RSS value is calculated based on the speed. If a node's RSS value is more than or equal to the threshold value, it is classified as a Sybil node.Otherwise, they are considered genuine nodes.



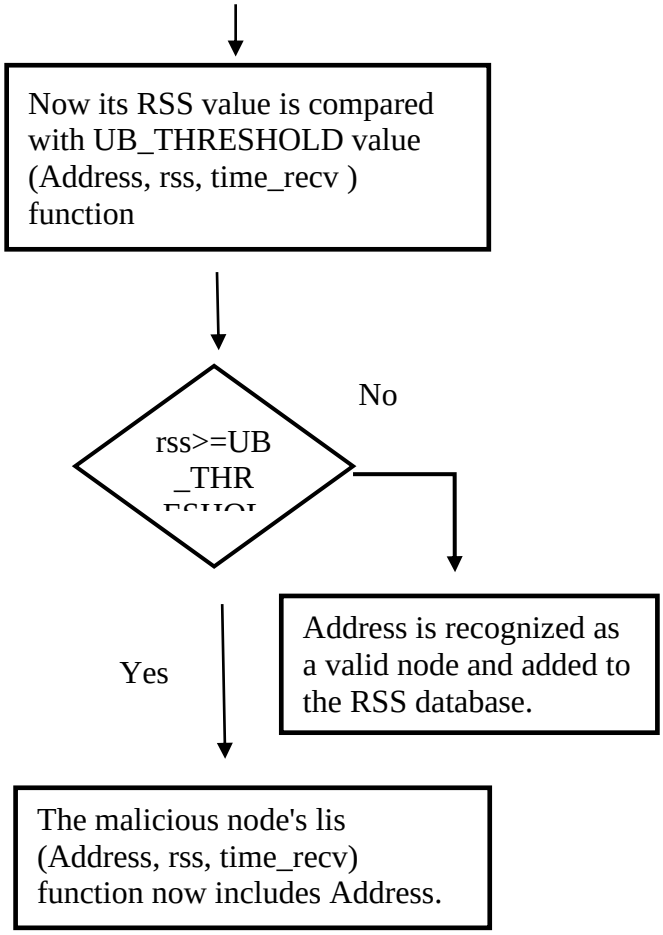


Fig 1.1:Diagram for the Simple lightweightSybil Attack Detection Algorithm

II. ALGORITHM

Input: Network size, Number Sensor Nodes (*M*), Number of Observation Nodes (*N*), Coverage Range (*R*), Transmission Power in db (*Ptx*), Speed Threshold (*Sth*)

Output: Set of Sybil Id's

Initialization

1. Construct a blank network with given input size.
2. Create arbitrary (x,y) positions for every node.
3. Distribute every Sensor node to randomly selected areas.
4. Deploy Observation nodes at logical locations

Simulation Stage

Loop for each Sensor Node

5. Generate random signal for each sensor node with input Transmission Power in db (*Ptx*),
6. Broadcast signal to each observation node in the network.

Measurement Stage

Loop for each Observation Node

7. Measure strength of received signal from each sensor node.

RSSI(i,j)=Received signal by ith Observation Node of jth Sensor Node.

Calculation Stage

Loop for each Sensor Node

8. *For* i=1 to total number of Sensor nodes

Estimate the current from measured received signal strength.

$$Current\ Location = X_i\ Y_i$$

Estimate the Speed of Sensor Node from Current Location and Old Location .

$$Displacement(d) = \sqrt{(X_i - X_i^{'})^2 + (X_i - X_i^{'})^2 m}$$

$$Speed = \frac{Displacement(d)}{Sample\ time\ of\ new\ location\ calculation}\ m/Sec^2$$

Update Old location with new locations,

$$Old\ Location = Current\ Location$$

End

Sybil Node Identification Stage

9. Calculate difference in estimated distance of each sensor node Δd

10. Identify Sybil node by following condition

$$\text{Sybil Node} = \begin{cases} False, & Speed < (Sth) \\ True, & Speed \geq (Sth) \end{cases}$$

III.RESULT

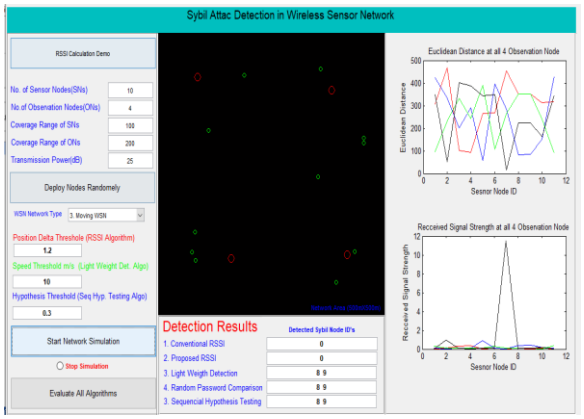
As a means of addressing the issue of Sybil node identification in moving wireless sensor networks (WSN), we conducted an evaluation of a lightweight Sybil node detection approach. This method needed much less resources for detection in comparison to encryption-based methods. Despite this, we discovered that the method showed promise in moving WSN.

This test based on WSN type

1. Moving WNS

Input details for All WSN Type –

1. No Of sensor Nodes(SNs)-10
2. Transmission Power (db)-25
3. Coverage Range of SNs-100
4. Converge Range of Ons-200



IV. CONCLUDING REMARKS

Automatic threshold selection or threshold Learning may be utilized with lightweight methods to get better detection accuracy with less resources. To be more effective in low-cost wireless sensor networks, this technique has to be optimized for the needs of the network. It is necessary to give the Random Password Comparison method further thought.

V. REFERENCES

[1]. P. Raghu Vamsi and Krishna Kant, "A Lightweight Sybil Attack Detection Frameworkfor Wireless Sensor Networks", IEEE(Aug 2014)

[2]. Abdolreza Andalib,Mojtaba Jamshidi, "A Lightweight Algorithm for Detecting Sybil Attack inMobile Wireless Sensor Networks using Sink Nodes", International Journal of Computer Applications Technology and Research(July 2016)

[3]. Mojtaba Jamshidi, Ehsan Zangeneh, Mehdi Esnaashari, Mohammad Reza Meybodi, "A lightweight algorithm for detecting mobile Sybil nodes in mobile wireless sensor networks", Computers and Electrical Engineering 0 0 0 (2016) 1–13(Nov 2017)

[4]. Mohsin Mulla, Santosh Sambare, "Efficient Analysis of Lightweight Sybil Attack Detection Scheme in Mobile Ad hoc Networks" International Journal of Computer Applications(Jan 2015)

[5]. RoopaliGarg,Himika Sharma, "Comparison between Sybil Attack DetectionTechniques: Lightweight and Robust", International Journal of Advanced Research in Electrical,Electronics and Instrumentation Engineering(2016)

[6]. Palak, M-Tech Scholar, "Review on the various Sybil Attack Detection Techniques in Wireless Sensor Network", International Journal of Computer Applications(April 2017)

[7]. Reza Mortazavi, Maryam Rahbari, "Distributed Sybil Attack Detection in VANET", International Journal of Computer Applications(Sept 2014)

[8]. Shehnaz T. Patel, Nital H. Mistry, "Sybil Attack detection in WSN", ICECS(June 2019)

[9]. B. Keerthi Samhitha, Suja Cherukullapurath Mana, Jithina Jose, M. Mohith, L. Siva Chandhrahasa Reddy, "An Efficient Implementation of a Method to Detect Sybil Attacks in Vehicular Ad hoc Networks using Received Signal Strength Indicator", (Nov 2019)