© 2015 IJSRSET | Volume 1 | Issue 6 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Survey on Detection of Sybil Attack in Wireless Sensor Network

Mirali Khanderiya, Prof. Mital Panchal

Department of Information Technology, L. D. Engineering College, Ahmedabad, Gujarat, India

ABSTRACT

As in wireless networks, communication happens through open air, nodes are more vulnerable to attacks and hence security becomes a major concern. Wireless Sensor Networks (WSNs) has many different applications in today's world, but at the same time it is also open to many security threats. Sybil Attack is one of these attacks, where a node illegitimately claims multiple identities and uses those identities in the network. These Sybil nodes obtains multiple fake identities, and pretends to be multiple, distinct nodes in the network. A Sybil node can disrupt the functioning and operation of network and may cause damage to the system if not detected. This paper analysis the existing detection schemes of Sybil attack in wireless networks, and the analysis and conclusion would be helpful in for obtaining a method that could detect Sybil attack overcoming all the existing scheme's limitations.

Keywords: Lightweight framework; multiple identities; RSSI; Sybil Attack; Wireless Sensor Networks (WSNs)

I. INTRODUCTION

Wireless Sensor Networks consists of large number of Wireless Sensor Nodes that are distributed over the network, to monitor, capture or measure physical or environmental conditions such as humidity, temperature, sound, pressure, etc.

WSNs are emerging on a large scale now-a-days. Because of their wireless configuration, they can be used in vast field of applications such as military, medical, building monitoring and control, automotive, traffic monitoring, industrial process control, open space surveillance, their range of application being practically unlimited [3].

Specific features of SNs in WSNs like the use of the broadcast medium, lack of tamper proof bodies, unattended and hostile deployment etc., often lead to physical capturing, vulnerabilities and security attacks [5].

Sybil Attack is a harmful threat to Sensor Network in which a sensor node has multiple identities. A Sybil node can illegitimately pretend to be multiple nodes with different fake identities using only single physical sensor node. Aim of Sybil node is to disturb the normal functioning and operations of the network.

II. METHODS AND MATERIAL

1. ASPECTS OF SYBIL ATTACK

A. Direct Vs. Indirect Communication[6]

In the former one, Sybil node directly communicates with the legitimate node, while in latter one the communication between them occurs through some malicious node.

B. Fabricated Vs. Stolen Identities[6]

In former case, Sybil node randomly creates various identities and broadcasts the massage using them, suppose the network has 32 bits address, then malicious node generates 32 bit identities and use them.

While in latter case, Sybil nodes identify the legitimate identities and use them maliciously. The attack would go undisclosed if the stolen identity node is already destroyed.

C. Simultaneous Vs. Non-Simultaneous[6]

Sybil node uses all its malicious identities at a time and pretends to be multiple nodes using single node simultaneously. While in other type the malicious node would change its identity with time but uses single identity at a time.

2. EFFECTS OF SYBIL ATTACK ON NETWORK

A. Data Aggregation

In some network, if there are enough illegitimate identities with a Sybil node than it can alter aggregate reading completely to whatever it desires.

B. Voting

Voting is used in many tasks in Wireless Sensor Networks, depending on number of identities a sensor node has, it can know the outcome of any voting operation well in advance & may even change it as per its requirement.

C. Fair Resource Allocation

When the resources are shared among nodes in per-node manner, a Sybil node pretending to be multiple nodes may acquire an unfair share of resources, claiming resources for each fake identity it owns. It might cause Denial of service (DoS) to some legitimate node, and creates the Sybil node more powerful.

D. Misbehaviour Detection

An attacker with many Sybil nodes could “spread the blame”, by not having any one Sybil identity misbehave enough for the system to take action. If the action taken is to revoke the offending node, the attacker can simply continue using new Sybil identities to misbehave, never getting revoked him. [6].

3. LITERATURE REVIEW

A. IPTTA: Leveraging Token-Based Node IP Assignment and Verification for WSN[1]

It is a node level authentication scheme where static unique IP address & dynamic unique token values are assigned to each node in the network.

For some network G, IP address to node **Ni** is assigned **A.B.M.M** from BS (Base Station).

Where, A=192, B=168, M= 1 to m,
m is total number of nodes.

In the same manner unique dynamic token is also assigned to each node for more security. When node joins network it is assigned both IP address and unique token.

Preceding operation, the BS chooses the trusted hubs for appointing hub IPs and builds mystery tokens with them. The BS produces the framework parameters to be distributed and gives those hubs the parameters for hub IP task.

Before node N_i and N_j communicate, there IP address and token are validated. If they are valid then communication continues else the node that is found to have address or token as invalid is considered as malicious.

In this paper the proposed approach IPTTA verifies the node IP and token, & fetches the contradictory node as Sybil node.

B. Efficient Analysis of Lightweight Sybil Attack Detection Scheme[2]

This method is based on use of RSS (Received Signal Strength) to detect Sybil attacker. It uses the RSS in order to differentiate between the legitimate and Sybil identities. First step is: Each node saves RSS information about neighbour nodes in the form of <Address, Rss-List <time, rss>> in a table. Next step is exposer of Sybil node, in which, assumption is made that all the legitimate node would have speed up to 10m/s i.e. the speed threshold. Accordingly RSS threshold is calculated say it, UB−THRESHOLD. Now RSS value of received signal is compared with UB−THRESHOLD, if RSS is greater than or equal to this value than that node are detected as Sybil node.

Nodes may join and leave the network at any point of time; hence nodes that exit from the network, eventually leaves a record of their RSS histories.

To control the size of record, a global timer, named RSS−TIMEOUT is plot in Algorithm, and it deletes unwanted records. When this timer expires, the rssTableCheck function gets called, which in return checks the time of last received RSS against the TIME−THRESHOLD for each and every address of the RSS table. If the time obtained is too much than threshold, indicates that more time has elapsed since last node heard, Now again the strength of the last RSS obtained is checked against the UB−THRESHOLD, if it is large, it indicates that it is the previous identity of an attacker; otherwise it is stated as an out of range scenario.

The only limitation of this method is that high end to end delay as compared to normal network condition which is the future work for this research.

C. Sybil Attack Type Detection in Wireless Sensor Networks based on Received Signal Strength Indicator detection scheme [3]

This paper presents a robust and lightweight solution to detect Sybil attack using RSSI (Received Signal strength Indicator).

Suppose node i receives a signal from node 0, the RSSI value is written as:

$$\text{Ri} = P_0 \text{K} / d_i^{\alpha}$$

With P0 transmitting power, Ri is RSSI, K is a constant, di is the Euclidean distance and α is the distance power gradient.

To use RSSI value of received signal, for deciding if its Sybil node is not advisable, because attacker might change its transmission power and send massage with different identity from same position. But the RSSI value would be different as it is dependent on transmission power of the signal.

For that in this paper an experimental setup is created, where we consider three detectors D1, D2, D3 and a Sybil node. We assume that the locations of D1, D2, D3, and the Sybil node are fixed, and then it is possible to detect the Sybil attack just by recording and comparing the ratio of the RSSI from the receivers.

In this setup we use the ratio of RSSI values. The ratio of RSSI for node i to j is can be written as:

$$\frac{\mathrm{R_i}}{\mathrm{R_j}} = \left(\frac{\mathrm{P_0\ K}}{\mathrm{d_i}^{\alpha}}\right) / \left(\frac{\mathrm{P_0\ K}}{\mathrm{dj}^{\alpha}}\right) = \left(\frac{d_i^{\alpha}}{d_j^{\alpha}}\right) \qquad \ldots(1)$$

Here they denote S1 and S2 as forged identities of Sybil node. Using S1 identity it broadcasts message at time t1 and using S2 it broadcasts at time t2.

All the detectors would listen to the messages that are broadcasted, and store the RSSI value and its respective identities. Detector D2 and D3 would send this stored data to D1.

D1 takes ratio of them shown in equations bellow.

$$\frac{R_{D1}^{S1}}{R_{D2}^{S1}}, \quad \frac{R_{D1}^{S1}}{R_{D3}^{S1}} \qquad ..(2)$$

$$\frac{R_{D1}^{S2}}{R_{D2}^{S2}}, \quad \frac{R_{D1}^{S2}}{R_{D3}^{S2}} \qquad ..(3)$$

If the ratios difference is near 0, then it concludes that a Sybil attack occurred because the same ratios means the transmitter is at the same location and only transmits multiple IDs as can be seen from the equation:

$$\frac{R_{D1}^{S1}}{R_{D2}^{S1}} = \frac{R_{D1}^{S2}}{R_{D2}^{S2}} \quad \text{And} \quad \frac{R_{D1}^{S1}}{R_{D3}^{S1}} = \frac{R_{D1}^{S2}}{R_{D3}^{S2}} \qquad ..(4)$$

RSSI was not considered stable in many papers, so in this paper experimentally it is showed that RSSI is stable enough for security mechanism in Zigbee protocol.

D. Sybil Attack Detection using Sequential Hypothesis Testing in Wireless Sensor Networks [4]

In this paper author proposes a method for detecting malicious node that falsify its identity and location information using sequential hypothesis testing (SHT).

In SHT, a node can accept a hypothesis from two competing hypotheses:
HO (null): neighbouring node is not a Sybil node,
HI (alternate): neighbouring node is a Sybil node.

Having observations of activities carried out by neighbouring nodes, a node computes a test statistic T(x) and compares it against two thresholds tl and t2 respectively to decide among three alternatives.

i. Acceptance of the null hypothesis if T(x) < tl.
ii. Acceptance of the alternate hypothesis if T(x) > t2.
iii. Computing test statistic one more time if tl < T(x) < t2.

In this, evidences are collected; evidence from direct observation and evidence from distance estimation are obtained. Collected evidence value called consolidated value is obtained by XOR of direct observation and distance estimation. The result would be a binary value. So using this consolidated value malicious activity could be found out.

If consolidated evidence value is 1 then it means it is Sybil node. Because the two evidences: observed and estimated are both having different value. This means node is trying to falsify its location position.

This paper shows that this proposed method detects Sybil attack without having false impacts of false positive and false negative.

III. CONCLUSION

In this paper we have reviewed many different methods and schemes that are used for detecting Sybil attack. Past detection schemes like radio Resource testing, Random key predistribution, registration were all having costly setup. Methods in this paper have their own advantages and disadvantages. As a future work we would improve one of these methods.

IV. REFERENCES

[1] S.Sakthi Vinayagam, Dr.V.Parthasarathy, "IPTTA: Leveraging Token-Based Node IP Assignment and Verification for WSN", In 2014, IEEE

[2] Mohsin Mulla, Santosh Sambare, "Efficient Analysis of Lightweight Sybil Attack Detection Scheme", In 2015,IEEE.

[3] Salavat Marian, Popa Mircea, "Sybil Attack Type Detection in Wireless Sensor Networks based on RSSI detection scheme", In 2015,IEEE.

[4] P. Raghu Vamsi and Krishna Kant, "Sybil Attack Detection using Sequential Hypothesis Testing in Wireless Sensor Networks", In 2014,IEEE.

[5] P. Raghu Vamsi and Krishna Kant, "Lightweight Sybil Attack Detection Framework for Wireless Sensor Networks", In 2014,IEEE.

[6] James Newsome, Elaine Shi, Dawn Song, Adrian Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses" In 2004, ACM.