© 2016 IJSRSET | Volume 2 | Issue 3 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Novel Approach for Detection of Sybil Attack in Wireless Sensor Networks

Mirali Khanderiya, Prof. Mital Panchal

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

ABSTRACT

Wireless Sensor Networks (WSNs) have gained tremendous popularity and importance in today's world due to their simple technology and versatility of applications. Due to their wireless configurations, , 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, and many more. In wireless networks, communication happens through open air, so nodes are more vulnerable to attacks, and hence security becomes a major concern. Wireless Sensor Networks has many different applications, but at the same time they are also open to many security threats. Security Attacks like Black hole attack, wormhole, etc., 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. In this work analysis of the existing detection schemes of Sybil attack in wireless networks is done. Researchers have developed many schemes and methodologies for detecting and preventing Sybil attack, but these security mechanisms are not being used satisfactorily in real scenario for Wireless Sensor Networks. In the proposed work I have tried to give a method that could detect Sybil attack.

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

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are emerging on a very large scale now-a-days. They consists of large number of Wireless Sensor Nodes(SNs) that are distributed over the networks, for monitoring, capturing or measuring physical or environmental conditions such as humidity, temperature, sound, pressure, etc. Wireless Sensor Networks have revolutionized in the fields of remote sensing, target tracking and monitoring. They are used for the transmission of the sensor output data to the control station, and thereby avoiding the adversities that are found in wired networks. Wireless sensor networks have recently come into prominence due to their potential to revolutionize many segments of our economy and life, environmental monitoring and conservation, target tracking, automation and industrialization and medical applications.

Wireless Sensor Networks has many different applications, but at the same time they are also open to many security threats. Security Attacks like Black hole attack, wormhole, etc., Sybil Attack is one of these attacks. 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 many fake identities using only single physical sensor node. Aim of Sybil node is to disturb the normal functioning and operations of the network. Malicious device's additional identities are called Sybil node.

II. METHODS AND MATERIAL

A. Aspects of Sybil Attack

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.

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.

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.

B. Existing Approach

Literature review is performed for this problem statement, and many approaches are studied. Authors have presented various methods for detection and/or prevention of Sybil Attack in Wireless Sensor Network.
In [3], author presents a robust and lightweight solution to detect Sybil attack using RSSI (Received Signal strength Indicator). For any node i, that receives a signal from node 0, the RSSI is

$$Ri = P_0 \, K \div d_i^{\alpha}$$

Where, P0 is transmitting power,
Ri is RSSI
di is distance
K is constant
α is distance gradient.

The methodology used by author in [3] is that it uses three detectors for detection of Sybil Node. For Scenario given in fig,

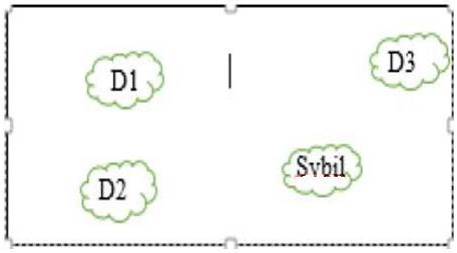

Figure 1: Scenario for existing Methodology

In this scenario, if Sybil node forges ID S1 & S2, and broadcasts packets using these identities at time t1 & t2 respectively. All three detector, measure RSSI value. Detector D2 and D3 would send this stored data to D1. D1 takes ratio of them shown in equations bellow.
At time t1 & t2,

$$\frac{R_{D1}^{S1}}{R_{D2}^{S1}}, \quad \frac{R_{D1}^{S1}}{R_{D3}^{S1}} \quad \& \quad \frac{R_{D1}^{S2}}{R_{D2}^{S2}}, \quad \frac{R_{D1}^{S2}}{R_{D3}^{S2}}$$

D1 now compares this ratio, if 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 through multiple IDs.

C. Issues in Existing Approach

In [3] RSSI value is used for detecting Sybil attack, but there three detectors were used for this scheme. Three detectors were required because the nodes that are at same distance from detecting node would have same RSSI value, so single node was not enough for detection process, as it would regard those nodes as Sybil too. Hence it would increase the false positive, so minimum three detectors were required.

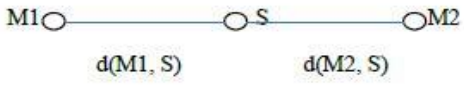

Figure 2: RSS from a single node is not sufficient

D. Proposed Methodology

A solution is proposed that works in two phases. Figure shows two phases of proposed solution.

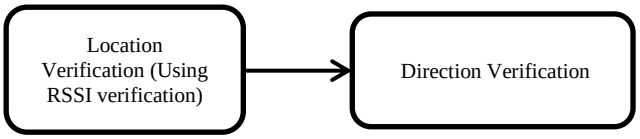

Figure 3: Block diagram of proposed methodology

Proposed model works with certain assumptions like: first, the network is static. Second, transmission power is fixed for both legitimate and Sybil node. In fact, these assumptions are all satisfied in current WSNs.[9]

According to the proposed solution, in the sensor network, the detector will maintain a table containing the list of RSS value and identity.

Workflow of the proposed system has the steps as follows:

When a packet is received, its identity is checked. If the identity is not found in the list, then it is Sybil node having fabricated identity.

Phase 1: If identity is found then RSS value is checked through following steps:

Step 1: Rss value would be computed for that received packet.

Step 2: Computed RSS value and identity pair would be compared to stored identities and respective RSS value.

Step 3: If RSS value does not match for that identity, then node detected as Sybil. Otherwise, same distance RSS match is performed (Step 4).

Step 4: Now if the RSS value of any identity other than the identity of received signal matches to it, then there might be Sybil node in the network and these two identities goes through second phase of the algorithm. Otherwise the nodes are legitimate and the data is proposed.

Step 5: Now for those that identity direction verification is performed.

Phase 2: In direction verification, the angle of received signal is found with reference to horizontal.

Step 1: Obtained Angle is compared with the angle that the identity should make with horizontal which is stored in the list.

Step 2: If angle matches then the received signal is from legitimate node, and sink node can process data.

Else the data is considered to be sent from a Sybil node and its packet information would not be processed or considered in the network operation.

Flow-chart of proposed solution

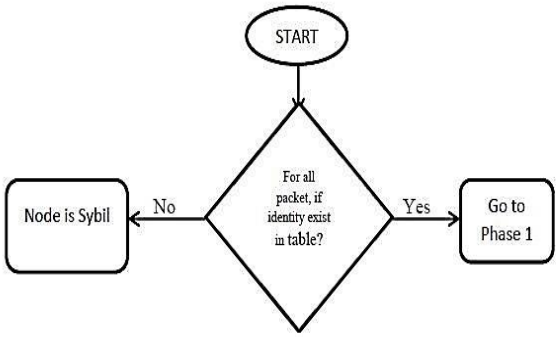

Figure 4: Flow-Chart of proposed solution

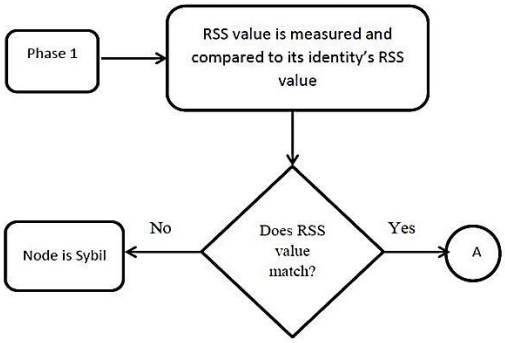

Figure 5 : Flow-Chart of proposed solution – Phase 1(I)

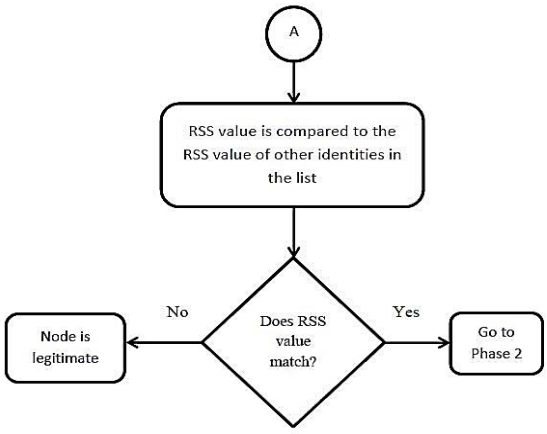

Figure 6: Flow-Chart of proposed solution – Phase 1(II)

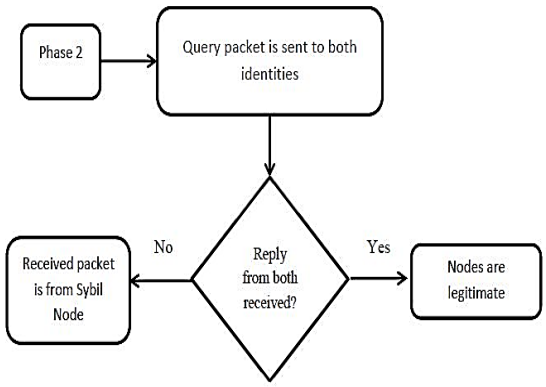

Figure 7: Flow-Chart of proposed solution – Phase 2

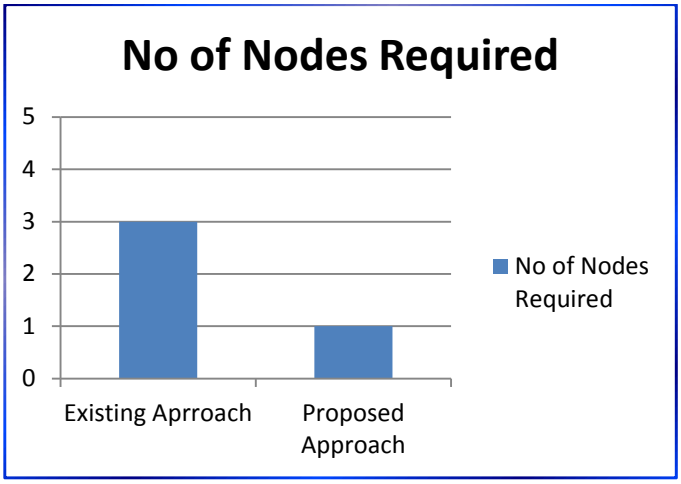

Figure 8 : Comparison of Approaches

III. RESULTS AND DISCUSSION

Implementation and Analysis

In this paper, the analysis of simulation in normal condition of network and after the Sybil attack created condition is performed and reported. The routing protocol used is AODV. The simulation parameters are shown in table. We have used NS-2.35 simulator for simulation. NS-2 works at packet level.

Table 1: Simulation Parameter

Parameters	Values
Simulator	NS2(2.35)
Routing Protocol	AODV
Transmission Range	250m
No. of Nodes	5, 10
No. of malicious Node	1,2

The proposed method detects Sybil attack successfully. The important point of comparison of proposed methodology and Existing System is that, existing system uses three detectors for detection of Sybil Node, while in the proposed methodology only single node is capable of identifying whether the received packet is sent from a legitimate node or a Sybil Node.

IV. CONCLUSION

In this paper, a methodology is proposed that is used to detect Sybil attack in wireless sensor network. Our proposed method uses AODV protocol; it has two phases for detection. It decides for every packet if the packet is sent from Sybil node or not. For every received packet this two phases are checked. And thereby, it prevents the illegitimate node from disturbing network's operation by participating as different legitimate identities. This approach requires only single node for detecting Sybil attack and thereby extends the future work of [3]. The approach is efficient as node power consumption is major issue in Wireless Sensor Network, as it has limited battery life. So, in this only one node works on detection algorithm. Hence it is energy efficient, requires single node.

V. REFERENCES

[1] S.Sakthi Vinayagam, Dr.V.Parthasarathy, "IPTTA: Leveraging Token-Based Node IP Assignment and Verification for WSN", 2014, IEEE. International Conference on Science, Engineering and Management Research

[2] Mohsin Mulla, Santosh Sambare, "Efficient Analysis of Lightweight Sybil Attack Detection Scheme", 2015, IEEE, International Conference on Pervasive Computing (ICPC)

[3] Salavat Marian, Popa Mircea, "Sybil Attack Type Detection in Wireless Sensor Networks based on Received Signal Strength Indicator detection scheme", 2015, IEEE Conference Publications

[4] P. Raghu Vamsi and Krishna Kant, "Sybil Attack Detection using Sequential Hypothesis Testing in Wireless Sensor Networks", 2014, IEEE. International Conference on Signal Propagation and Computer Technology (ICSPCT).
[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: ACM, Proceedings of the International Symposium on Information Processing in Sensor Networks, April 2004
[7] Mirali Khanderiya, Prof. Mital Panchal, "A Survey on Detection of Sybil Attack in Wireless Sensor Network"
[8] Murat Demirbas, Youngwhan Song, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks", WOWMOM '06 Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks
[9] Shaohe Lv, Xiaodong Wang, Xin Zhao and Xingming Zhou "Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks", In : 2008, IEEE. International Conference on Computational Intelligence and Security
[10] Pooja, Manisha, Dr. Yudhvir Singh "Security Issues and Sybil Attack in Wireless Sensor Networks" In : International Journal of P2P Network Trends and Technology