Middle-East Journal of Scientific Research 23 (Sensing, Signal Processing and Security): 202-206, 2015
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2015.23.ssps.55

Detection of Sybil Attack in Wireless Sensor Network

[1]V. Sujatha and [2]E.A. Mary Anita

[1]Department of Computer Applications, S.A.Engineering College, Chennai, India
[1]Research Scholar, AMET University, Chennai, India
[2]Professor, Department of CSE, S.A. Engineering College, Chennai, India

Abstract: In Wireless networks the legitimacy and uniqueness is essential due to the broadcast nature of wireless medium. In this paper, we investigate Sybil attack which is one of the most disrupting attacks in the context of wireless sensor networks. In this attack, a node illegitimately asserts numerous characters and acquires multiple identities and performs as the original nodes causing disrupts in routing, voting, data leakage and data aggregation. A lightweight scheme is proposed to detect the new identities of Sybil nodes without using centralized trusted third party and our scheme utilizes neighborhood RSS to differentiate between the legitimate and Sybil identities.

Key words: Sybil attack · Sensor Network · Throughput · Delay

INTRODUCTION

Wireless Sensor Networks (WSN)are heterogeneous systems consisting of hundreds and thousands of self-organizing spatially distributed autonomous nodes. As wireless networks are adopted in diverse environments and applications, the focus is on routing security. The security has become one of their top priorities. The uniqueness and legitimacy of the node identity must be imposed to facilitate the primary operations like routing, resource allocation and misbehavior detection.

In this paper, we focus on the Sybil attack which is to denote an attack where the Sybil node claims multiple identities or claims fake IDs. Due to this attack, the node replicates itself to confuse the network. In WSN, a Sybil attacker can change the aggregated analysis of outcome by acting or subsidizing many times as a different node. Sybil attacker being an inside and passive attacker, it is desirable to detect the Sybil attack in order to eliminate them.

A Sybil attacker can disturb the location-based routing by participating in the routing, giving the fake impression of being individual nodes on different locations. The Sybil attack detection process can also be implied with use of cryptographic authentication but this incurs overhead since the maintenance of random keys is difficult. This paper implements a Sybil attack detection technique based on using ratios of RSSIs from multiple nodes. The technique was first introduced by Sohail Abbas *et al.* [1] as a localization solution in mobile adhoc networks and this is now extended to WSN. This method presents a robust and lightweight solution for Sybil attack problem based on received signal strength indicator (RSSI) readings of messages.

Related Work: Chris Piro, *et al.* [2] have proposed that the mobility of nodes in a wireless network can be used to detect and identify nodes that are part of a Sybil attack. Two methods have been proposed which can run on standard, inexpensive equipment without any special antennae or hardware and with only very loose clock synchronization.

M. Merabit *et al.* [3] suggest that nodes can locally determine their locations through received signal strength variations and inform the neighbors about the location updates automatically.

Raghu Vamsi P, *et al.* [4] have proposed a lightweight Sybil attack detection framework which consists of evidence collection and validation. Every node in the network collects the evidences by observing the activities of neighboring nodes. These evidences are validated by running sequential hypothesis test to decide whether neighboring node is a Sybil node or not.

Corresponding Author: V. Sujatha, Department of Computer Applications,
S.A. Engineering College, Chennai, India. E-mail: sujathasheik@yahoo.co.in.

Sohail Abbas, *et al.* [5] have proposed a method for preventing whitewashing attack by one-time location information at the time when new nodes join the network which substantially reduces the overhead incurred by periodic dissemination of location information.

Xiaoyazhu *et al.* [6] address Sybil attack by a RSSI-based distributed detection mechanisms. In this the protocol is designed on MAC layer, so as to run on WSN systems with different routing protocols. Location based solutions are the most important problems in which the node self-localization causes lot of communication overhead and computation.

Yingyingchen, *et al.* [7] have proposed a method for detecting both spoofing and Sybil attacks with high detection rate and a low false-positive rate, thereby providing strong evidence of the effectiveness of the attack detector utilizing the spatial correlation of RSS and the attack localizer.

Yingyingchen, *et al.* [8] have proposed a method for both detecting spoofing attacks as well as locating the positions of adversaries performing the attacks. This approach utilizes the Received Signal Strength (RSS) measured across a set of access points to perform spoofing detection and localization.

Proposed Work: A light weight scheme is proposed to detect the Sybil identity without using third parties. In particular, the scheme uses the RSS in order to differentiate between the legitimate and Sybil node. This method detects all Sybil attack cases with very little false-positives.

Let S be a set of n sensor nodes deployed in a geographical region. These nodes interact directly with each other to forward the packet. It adopts that each node has a unique identity and is aware of its own location. Each node makes use of promiscuous mode of the network interface. This strategy detects every new identity created by a Sybil attacker. The two types of Sybil attack has been defined, In the first type, the attacker creates new identity while discarding the previously created one, thereby having only one identity of the attacker at a time in the network. The Figure 1 shows the System Architecture.

This is called as join-and-leave attack. In the other type, the attacker concurrently uses all its identities for an attack which is called as simultaneous Sybil attack. In the network, each node maintains a neighbor table to store information associated with their neighbors. If the information consists of identity of the node and location, then the receiving node shall compute the distance

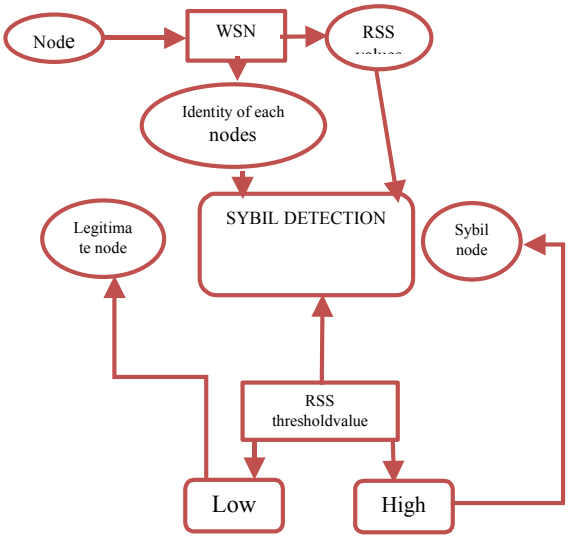

Fig. 1: System Architecture.

between the nodes, RSS and store them in the neighbor table. After a certain time of network operation, an adversary captures and alters one or more legitimate nodes and places back in the network. These nodes try to convert its neighboring nodes as malicious ones. The signal strength of the newly created identity will be high so that it cannot be distinguished from the newly joined neighbor. The greater the transmission rate of the node, earlier their presence will be acknowledged and vice versa.

The distinction between the Sybil node and a legitimate node can be estimated using the signal strength. Also, each node captures and stores the signal strength of the transmissions received from neighboring nodes. Detection of threshold values are nothing but the smallest readable RSS values. Detection threshold values are set up based on the RSS threshold values like If RSSs from newcomers is greater than the threshold which imply abnormal entry into the neighborhood. In this case, it checks the identity of both nodes. If the node identity for both nodes are the same, then it checks for the RSS values of both the nodes. If it is greater than or equal to the threshold, which indicates that the new node lies near in the neighborhood and its entry is not normal into the neighborhood. Its address is added to the malicious node list.

Otherwise, the address is added to the RSS table and a link list is created in order to store the received RSS. Finally, the size of the link list is checked to see if it is greater than LIST-SIZE. If so, the old RSS is removed from the list. If the RSS values of any one of the node is greater than the other node, then it is considered as the Sybil node.

Algorithm:
addNewRSS (Address, rss, time-recv)
BEGIN SUB:
IF: Address is not in the Table
THEN:
IF: rss>=UB-THRESHOLD
THEN: Add-to-Malicious –list(Address)
Bcast-Detection-Update(Address)
ELSE: Add-to-Table(Address)
END-IF
Create-Record(Address)
Push-back(rss, time-recv)
IF: list-Size> LIST-SIZE
THEN: Pop-front()
END SUB:

Simulation: Consider the set of n sensor nodes being static, deployed in a geographical region. These nodes interact directly with each other to forward the packet. It is assumed that each node has a unique identity and is aware of its own location.

First all these static nodes are arranged in a particular topology and start to communicate with each other. The identity and RSS values of each nodes are identified and a particular RSS_threshold value is noted.

The RSS value of each node is noted in order to differentiate the normal node and a Sybil node.
The Figure 2 shows the calculation of RSS.

The comparison of all node identity are taken and stored. If these values are the same, then the RSS values of the node is checked with the threshold values which have already been taken. If the value is greater, then it is considered as a Sybil node.
Figure 3 shows the detection of Sybil node.

If the value is lesser or equal to the threshold value then it is regarded as a legitimate node. Figure 4 Shows Sybil nodes.

The comparisons are made with the parameters namely: Throughput, end-to-end delay, packet-loss ratio, true positive rates and false positive rates.

Throughput: Throughput denotes the rate of successful delivery.

Figure 5 shows the comparison of the throughput in the presence of Sybil node and in the absence of the Sybil node. The throughput decreases in the presence of Sybil node. As the packets that are routed decrease, the throughput value decreases and vice versa.

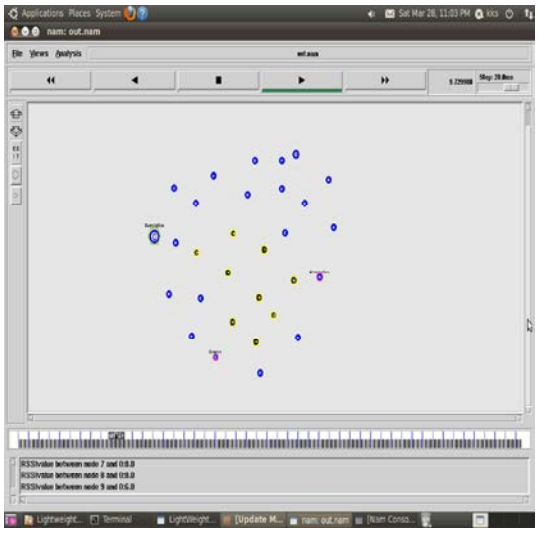

Fig. 2: Calculation of RSS

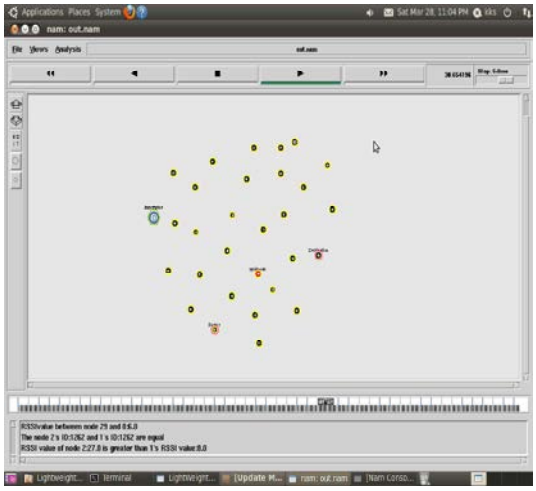

Fig. 3: Detection of Sybil node

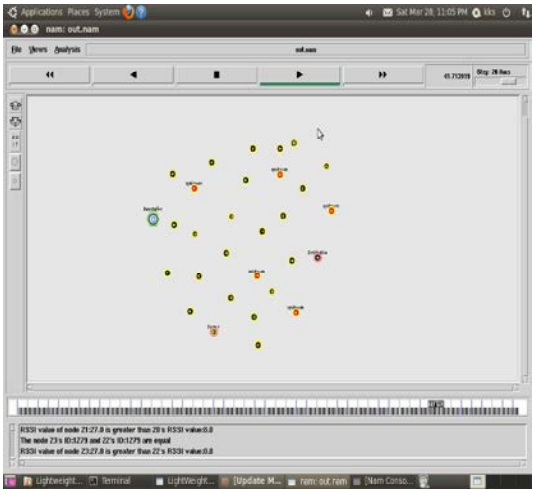

Fig. 4: Sybil nodes

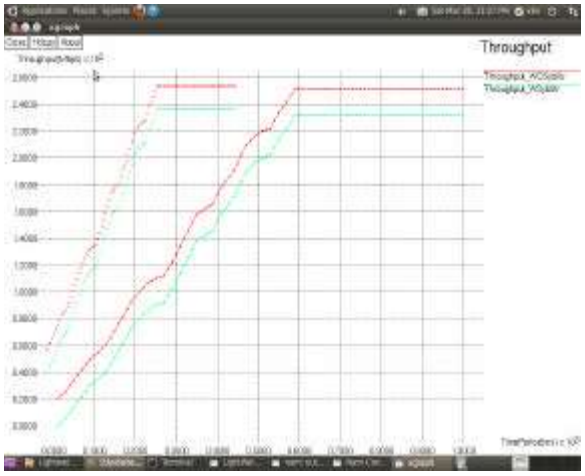

Fig. 5: Throughput with and without Sybil node

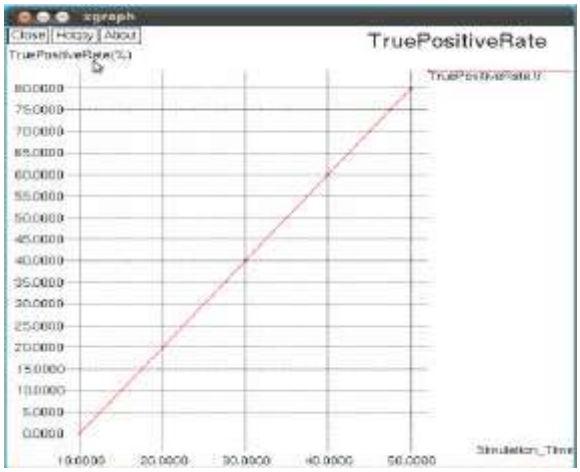

Fig. 7: True positive rate

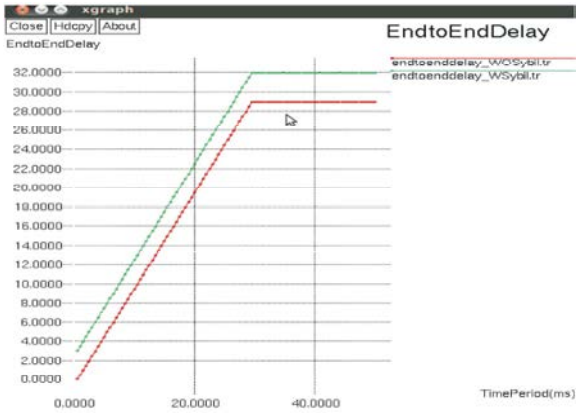

Fig. 6: End-to-End delay

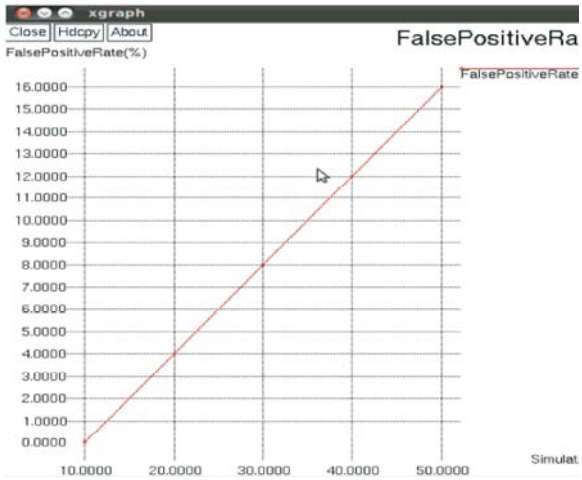

Fig. 8: False positive rate

End-to-end delay: End-to-end delay denotes the delay occurring during the transmission of each and every node.

Figure 6 shows the comparison of the end-to-end delay in the presence of Sybil node and in the absence of the Sybil node. As time increases the end-to-end delay will be more when there is a Sybil node and it will be less in the absence of the Sybil node.

True Positive Rate: True positive rate means a malicious node is correctly detected.

Figure 7 shows the True positive rates of the nodes in the network according to the simulation time. The true positive rate in the proposed scheme results up to 80%.

False Positive Rate: False positive rate means a malicious node is not detected correctly.

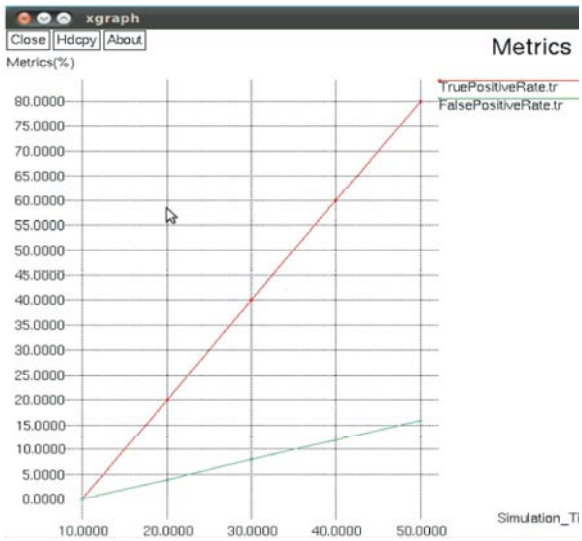

Fig. 9: Comparison of True positive and False positive rate

Figure 8 shows the false positive rate in the network. This value is compared with the simulation time. Hence in this network the false positive rate is up to (16%). False positive means a good or legitimate node is incorrectly detected as a malicious.

Figure 9 shows the comparison of true positive rate and the false positive rate with respect to the simulation time. Hence in this paper, the true positive result is up to 80% and the false positive rate is up to 16%.

In this paper the true positive result is more when compared to the result of the false positive. Hence this system is proposed with the good accuracy.

CONCLUSION

In this proposed scheme a RSS based process is used in wireless sensor network to detect Sybil attacks. It is verified that a detection threshold makes the distinction between legitimate new nodes and new malicious identities. The factors such as throughput, packet loss ratio, end-to-end delay, true positive rates, false positive rates analyze the performance of the system. The simulation results show that this scheme has a high level of accuracy. This detection process gives us the high true positive rates up to 80% and the low false positive rates that ranges to 16%.

REFERENCES

1. Sohail Abbas, MadjidMerabti, David Llewellyn-Jones and Kashif kifayat, 2013. “Lightweight Sybil Attack Detection in MANETs”, IEEE Systems Journal, 7(2), June 2013.
2. Chris Piro Clay Shields Brian Neil Levine, 2013. “Detecting the Sybil Attack in Mobile Adhoc Networks ”IEEE Communications Letters, 17(5), May 2013.
3. Merabit, M. and D. Llewellyn-Jones, 2009. “Signal Strength Based Sybil Attack Detection In Wireless AdhocNetworks”,IEEE Trans. Mobile Comput., 5(1): 43-51, Jan. 2009.
4. Raghu Vamsi, P. and Krishna Kant, 2014. “A Lightweight Sybil Attack Detection Framework For Wireless Sensor Networks”.
5. Sohail Abbas, Madjid Merabti and David Llewellyn-Jones, 2010. “Deterring Whitewashing Attacks in Reputation Based Schemes for Mobile Ad hoc Networks”.
6. Xiaoyazhu, Xianchun Zhou, 2013. “A Regional Statistics Detection Scheme Against Sybil Attacks In WSNs”, IEEETrans. Mobile Comput., 2(3): 257-269, Jul-Sep 2013.
7. Yingyingchen, JieYang, Richard p Martin and Wade Trappe, 2010. “ Detecting And Localizing Identity-Based Attacks In Wireless And Sensor Networks”.
8. Yingyingchen, Wade Trappe, Richard p Martin and Wade Trappe, 2010. “ Detecting And Localizing Wireless Spoofing Attacks” IEE Trans. Veh. Technol., 59(5): 2418-2434, Jun 2010.