Volume 3, Issue 12, December 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Study on Detection of Sybil Attack in Wireless Sensor Network

Anuja Motarwar
4th semester M.E. Computer Science & Engineering
G.H. Raisoni College of Engg.
Nagpur, India

Prof. Amresh Kumar
Computer Science& Engineering
G.H. Raisoni College of Engg.
Nagpur, India.

Abstract- As the technology improves the method of communication and reduces the network overhead it also opens a wide spectrum for attacker to break the security. As wireless communication happens through open air, it also increases possibility of fetching the information from air medium using sniffing software tools. A particularly harmful attack against sensor networks is known as the Sybil attack, where a node illegitimately claims multiple identities and simultaneously uses those identities in the network. In this paper we analyze fake identity in network which is created by Sybil attack by detecting its source. Analysis have found some solution that include the communication among the nodes of cluster and analyze the results in different scenarios like fake sender detection, fake receiver blocking, node to node secure connection and packet acceptance and rejection process.

Key words— Wireless sensor networks, Sybil attacks, Identity-based attacks, multiple identities, fake identity.

I. INTRODUCTION

The emergence of sensor networks as one of the dominant technology trends in the coming decades has posed numerous unique challenges to researchers. The development of wireless sensor networks was motivated by military applications such as battle field surveillance. The Sybil attack is a particularly harmful threat to sensor networks where a single sensor node illegitimately has multiple identities. A Sybil node may create an arbitrary number of additional node identities using only one physical device. The Sybil attack can disturb normal performance of the sensor network, such as the multipath routing, used to discover the multiple displace paths between sender-receiver pairs. But the Sybil attack can interrupt it when a single adversary presents several identities, which appear on the multiple paths. Researchers have proposed a light-weight identity certificate method to defeat Sybil attacks, but it is not suitable for a big scale sensor network because of the huge memory usage required at each node. A Sybil attacker can either create more than one identity on a single physical device in order to launch a coordinated attack on the network or can switch identities in order to weaken the detection process, thereby promoting lack of liability in the network. A Sybil attacker can cause damage to the ad hoc networks in several ways.

For example, a Sybil attacker can disrupt location-based or multipath routing by participating in the routing, giving the false impression of being distinct nodes on different locations or node-disjoint paths. In reputation and trust-based misbehaviour detection schemes, a Sybil node can disrupt the accuracy by increasing its reputation or trust and decreasing others' reputation or trust by exploiting its virtual identities. In wireless sensor networks, a Sybil attacker can change the whole aggregated reading outcome by contributing many times as a different node. In voting-based schemes, a Sybil attacker can control the result by rigging the polling process using multiple virtual identities. In vehicular ad hoc networks, Sybil attackers can create an arbitrary number of virtual non-existent vehicles and transmit false information in the network to give a fake impression of traffic congestion in order to divert traffic.

When a node illegitimately claims multiple identities or claims fake IDs, the WSN suffers from an attack called Sybil attack. External attacks can be prevented by authentication but not the inside attacks. There should be node to node mapping between identity and entity in WSN. But this attack violates this one-to-one mapping by creating multiple identities.

II. BACKGROUND

✓ Types of Sybil Attack

In order to detect the Sybil attack it is necessary to understand the different forms in which the network is attacked.

(a) Direct and Indirect Communication:

In direct attack, the legitimate nodes communicate directly with Sybil nodes whereas in indirect attack, communication is done through malicious node.

(b) Fabricated and stolen identities:

It creates a new identity for itself based on the identities of the legal nodes, that is, if legitimate nodes have identification with length 32 bit integer, it randomly creates identification of 32 bit integer. These nodes have fabricated identities.

In stolen identities, attacker identifies legitimate identities and then uses those identities. The attack may go undisclosed if the node whose identity has been stolen is destroyed. Identity replication is when the same identities are used many times in the same places.

(c) Simultaneous and non-simultaneous attack:

In simultaneous, all the Sybil identities participate in the network at the same time. Since only one identity appears at a time, practically cycling through identities will make it appear simultaneous.

The number of identities the attacker uses is equal to the number of physical devices; each device presents different identities at different times.

- ✓ **Sybil attack on protocols**

In a Sybil attack, a malicious node can generate and control a large number of identities on a single physical device. This gives the illusion to the network as if it were different legitimate nodes. It can affect the following important protocol.

Distributed Storage The Sybil attack affects the architecture where it replicates the data on several nodes. Data will be stored on Sybil identities.

Routing Routing mechanism in which the nodes are supposed to be disjoint is affected by Sybil identities because one node will be present in the various paths and different locations at the same time.

Data Aggregation In sensor networks, data is grouped into one node to form complete information. When a Sybil node contributes many times posing as different users, the aggregated data changes completely thus giving false information.

Voting In WSN, most of the decisions are made by voting system. Since the Sybil node has many identities, a single node has a many chance for vote, thus destructing the process.

Misbehaviour detection: A Sybil node increases the reputation, credit, trust value by using its virtual identities. Thus the accuracy to detect a malicious node is reduced.

Fair resource allocation: Since the Sybil node has multiple identities it affects the allocation of resources. For example, when many nodes share a single radio channel, each node will be assigned a fraction of time per interval during which they can broadcast. Since the Sybil node has many ID's, it can obtain an unfair share of the resources thus reducing the actual share of resources to the authorized node.

III. RELATED WORK

Present Detection Methods of Sybil attack:

(a) Radio resource testing:

Consider that a node wants to verify that none of its neighbours are Sybil identities. It can assign each of its neighbours a different channel to broadcast some message on. It can then choose a channel randomly on which to pay attention. If the neighbour that was assigned that path is legitimate, it should hear the message. Let's' be the total number of the nodes 'n' be the number of Sybil nodes. The probability of detecting the Sybil node is s/n.

A more difficult case is when there are not enough channels to assign each neighbour a separate channel. In this case, a node can only examine some subset of its neighbours at one time. If there are 'c' channels, then the node can test 'c' neighbours at once. Note that a malicious node not in the subset being tested can cover for a Sybil node that is being tested by transmitting on the channel that the Sybil node is supposed to be transmitting on.

(b) Registration:

One obvious way to prevent the Sybil attack is to perform identity registration. A difference between peer-to-peer networks and wireless sensor networks is that in wireless sensor networks, there may be a reliable central authority managing the network, and thus knowing deployed nodes. The trusted central authority may also be able to disseminate that information securely to the network. . To detect Sybil attacks, an entity could poll the network and compare the results to the known deployment. To prevent the Sybil attack, any node could check the list of "known-good'' identities to validate another node as legal node. Registration process is likely to be a good initial defence in many scenarios, with the following limitations. The list of known identities must be protected from being maliciously modified. If the attacker is able to add identities to this list, he will be able to create and add Sybil nodes to the network.

(c) Position Verification:

Another promising approach to defending against the Sybil attack is position authentication. Here assume that the sensor network is immobile once deployed. In this approach, the network verifies the physical position of each node.

Sybil nodes can be detected using this approach because they will appear to be at exactly the same position as the malicious node that creates them. By placing a limit on the number of nodes in the network, in-region verification can be used to tightly bind the number of Sybil identities that a malicious node can create.

(d) Based on RSSI:

By having the position of the nodes based on signal strength, we can find whether there is Sybil attack or not in wireless sensor networks. Initially all the nodes have the same power, computing capability and the positions of nodes are fixed. The network is safe when the nodes are initialized using the signal strength. The disadvantage is the nodes are time varying.

IV. PROPOSED METHODOLOGY

After the brief analysis on Sybil attack detection in wireless sensor network analysis result conclude that the best Sybil attack detection in network can be achieved by designing a special packet which include node's unique identity and encrypting the transmitted data by using node's unique identity. The proposed system deal with fake identity identification and preventing the Sybil attacks by detecting its source. Using encryption technique we can assure that only desired node can decrypt the data using its decryption key.

The proposed system has following concepts such as,

- Fake sender detection
- Fake receiver blocking
- Node to node secure connection
- Packet acceptance and rejection process

Fake sender detection: figure 2 describes the process where node will generate the signal and if the sender is authentic then only receiver will accept the data and display it on LCD screen or if sender is un-authentic then receiver will reject the data and acknowledge the receiver about the fake identity attack.

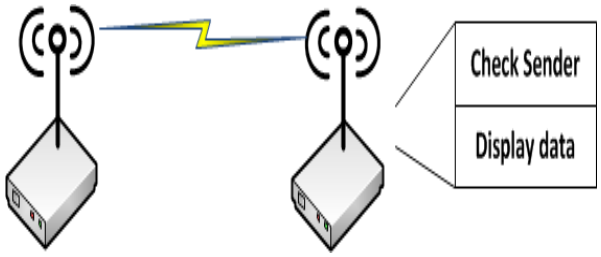

Fig.1. Fake Sender

Fake receiver data read blocking: In Figure 3 sender will generate the data which can be received by the entire node in the network but only authentic node with data decryption capability can read the data.

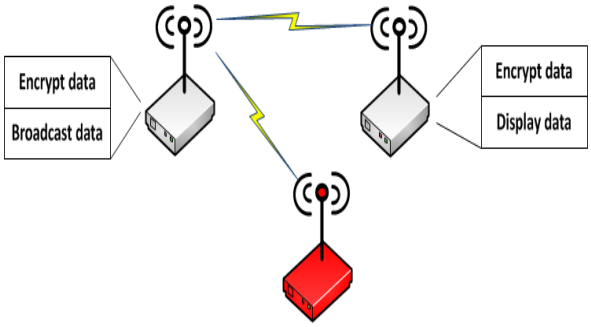

Fig.2. Fake Receiver

Research methodology to be employed-

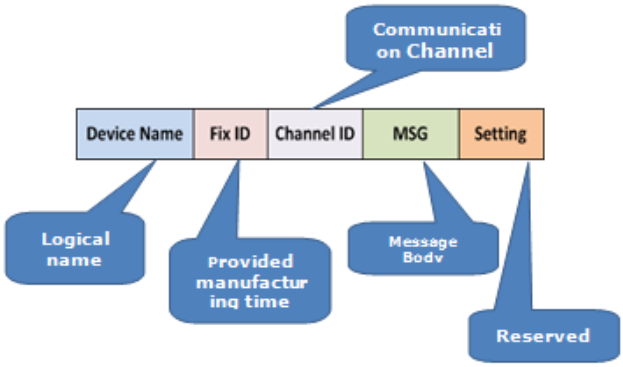

Fig.3. Data Packet

Figure 3 consist of packet structure which have several fields namely Device name is the logical name of the device, Fix ID which is provided at manufacturing time, Channel ID is the identity of channel on which communication is carried out, Data (message), Setting(if required).Packet is specially designed for providing the authentication to the system by using Fix ID. As this system provides efficient technique for detecting Sybil attack in wireless sensor network and eliminate the drawback of existing system this is best suited solution for achieving Sybil attack detection.

V. CONCLUSION

In this paper, we proposed a method for detection of identity based attack, Sybil attack. The method analyzes the result in different scenario such as Fake sender and Fake receiver blocking. Nodes discard data from the fake sender or in case of fake receiver; it cannot decrypt the data using its unique id. Unlike other traditional identity based authentication method, our scheme does not increase the overhead on sensor nodes.

REFERENCES

[1] J. Douceur. The Sybil Attack. In First International Workshop on Peer- to-Peer Systems, pages 251–260, 2002.

[2] R. C. Merkle. Secure Communications over Insecure Channels. Communications of the ACM, 21(4):294–299, 1978.

[3] J. Newsome, E. Shi, D. Song, and A. Perrig. The Sybil Attack in Sensor Networks: Analysis & Defenses. In International symposium on information processing in sensor networks, pages 259–268, 2004.

[4] 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.

[5] 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.

[6] M. Raya, P. Papadimitratos, and JP. Hubaux. Securing Vehicular Communications. IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, 13(5):8–15, 2006

[7] M. S. Bouassida, G. Guette, M. Shawky, and B. Ducourthial, "Sybil nodes detection based on received signal strength variations within VANET," Int. J. Netw. Security, vol. 8, pp. 322–333, May 2009.

[8] W. Pires, T. de Paula Figueiredo, HC. Wong, and A. Loureiro. Malicious Node Detection in Wireless Sensor Networks. In IEEE International Parallel & Distributed Processing Symposium, 2004.

[9] Bin Xiao, Bo Yu, and Chuanshan Gao. Detection and Localization of Sybil Nodes in VANETs. In ACM/SIGMOBILE Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks, pages 1–8, 2006.

[10] T. Suen and A. Yasinsac. Ad Hoc Network Security: Peer Identification and Authentication Using Signal Properties. In Systems, Man and Cybernetics (SMC) Information Assurance Workshop, pages 432–433, 2005.

[11] P. Golle, D. Greene, and J. Staddon. Detecting and Correcting Malicious Data in VANETS. In ACM international workshop on Vehicular ad hoc networks, pages 29–37, 2004

[12] A. Tangpong, G. Kesidis, H. Hung-Yuan, and A. Hurson, "Robust Sybil detection for MANETs," in Proc. 18th ICCCN 2009, pp. 1–6.

