DETECTION METHODS OF SYBIL ATTACK IN WIRELESS SENSOR NETWORKS

[1]Shaik Saleem, [2]Dr. Radhika Baskar

[1]Bachelor's Student, [2]Associate Professor
Department of Electronics and Communication Engineering,
Saveetha School of Engineering, SIMATS, Chennai, India

Abstract: **Wireless sensor networks are one of the real issues; consequently, inquire about is being done on many directing attacks on wireless sensor networks. This paper concentrates on Sybil attacks and its identification. At the point when a node misguidedly guarantees numerous identities or cases counterfeit id, is called Sybil attack. In this attack, a node misguidedly attests various characters, procures numerous identities, and executes as the first node causing upsets in directing, voting, data aggregation and Fare resource allocation. A Sybil attack is proposed to identify the new characters of Sybil nodes without utilizing concentrated trusted outsider and our plan uses Received signal strength, throughput, packet delivery ratio to separate between the genuine and Sybil identities.**

Keywords: **Wireless sensor networks (WSN), Sybil attack, and Sybil node detection.**

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have begun to assume an indispensable part of our day to day lives. It is a direct result of the decrease in cost of the sensor nodes, prompting expanding arrangements of WSNs to a larger degree. Potential applications for wireless sensor systems exist in an assortment of fields, including mechanical process observing and control, condition and living space checking, applications like nuclear reactor control, fire recognition, protest following and movement control. Productive outline and execution of wireless sensor network shave turned into a hot range of research lately, because of the enormous limit of sensor networks to empower applications associating the physical world with the virtual world. It is conceivable to get information about physical or ecological marvels by the networking substantial number of modest sensor nodes that was troublesome or difficult to acquire in more conventional ways.

2. SYBIL ATTACK

At the point when a node misguidedly guarantees different identities or cases counterfeit IDs, the WSN experiences an attack called Sybil attack. The node imitates itself to make many duplicates to confuse and crumple the network.

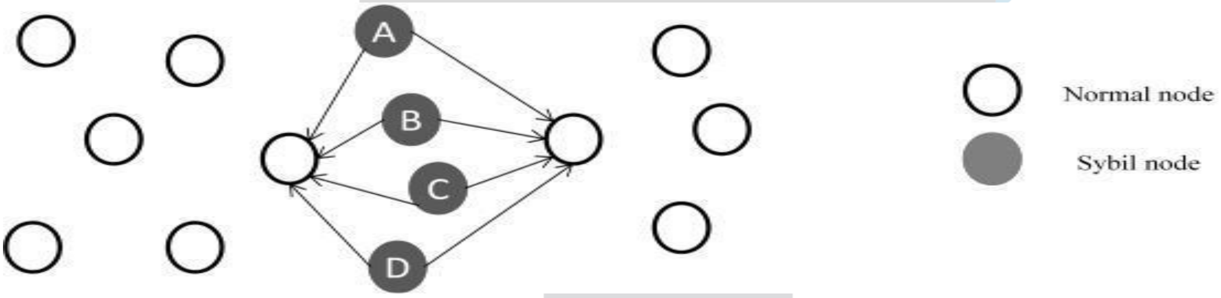

Fig 2.0 Sybil attack

From fig 2.0 A, B, C, D is the Sybil nodes. At the point when these nodes need to convey to their neighboring nodes they utilize any of the identities. This confuses and collapses the network.

There are some different methods in which the network is attacked in a wireless sensor network.

(a) **Direct and Indirect Communication track:** In a direct attack, the genuine nodes discuss specifically with Sybil node while in the circuitous attack, the correspondence is done through the malignant node.

(b) **Fabricated and stolen identities attack**: It makes another character for itself in light of the identities of the real nodes, that is, if honest to goodness nodes have an ID with length 32-bit whole number, it arbitrarily makes ID of 32-bit whole number. These nodes have manufactured characters.

In stolen characters, aggressor distinguishes genuine identities and afterward utilizes it. The attack may go unidentified if the node whose character has been stolen is crushed. Identity replication is the point at which similar characters are utilized commonly in similar places.

(c) **Simultaneous and non-simultaneous attack**:

In synchronous, all the Sybil identities take an interest in the network in the meantime. Since just a single character shows up at once, for all intents and purposes going through identities will influence it to seem concurrent.

The quantity of characters the assailant utilizes is equivalent to the number of physical gadgets; every gadget presents distinctive identities at different times.

2.1 Types of Sybil attack:

Different types Sybil attacks like data aggregation, voting, misbehavior detection and fare resource allocation.

2.1.1 Data aggregation:

In some network, if there are sufficient ill-conceived characters with a Sybil node than it can adjust total perusing totally to whatever it wants.

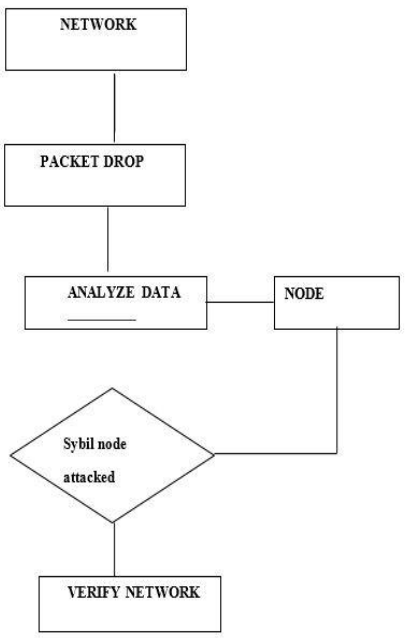

Fig: 2.0.1 Flow chart of Sybil attack

2.1.2 Voting:

Voting is utilized as a part of many undertakings in Wireless Sensor Networks, contingent upon number of identities a sensor node has, it can know the result of any voting operation well ahead of time and may even change it according to its requirement.

2.1.3. Misbehavior detection:

An attacker with numerous Sybil nodes could "spread the fault", by not having anyone Sybil identity act up enough for the framework to make a move. On the off chance that the move made is to deny the culpable node, the attacker can just keep utilizing new Sybil identities to act up, never getting disavowed him.

2.1.4 Fair resource allocation :

Since the Sybil node has numerous characters it influences the distribution of assets. For instance, when numerous nodes share a solitary radio channel, every node will be doled out a small amount of time per interim amid which they can transmit. Since the Sybil node has numerous identities, it can acquire an unjustifiable offer of the assets in this way decreasing the real offer of assets to the honest to good nodes.

2.2 METHODS ON DETECTING SYBIL ATTACK:

There are two ways to deal with managing the Sybil attack, for instance, coordinate approval and backhanded approval. coordinate approval is the node straight forwardly support another node. Aberrant approval expresses that node checks by another node, not specifically. Sybil attack nature has a number of Sybil node more critical than the standard node when one of the nodes has talked with another node by methods for broadcasting (Omni directional). So this case has been to recognize the malignant characters by social occasion information from neighboring node. Since various characters made by each node that it has suggested as Sybil node. Neighboring information is used to avoid the less respected status of ambushes in data aggregation and voting methods. The essential concern is to concentrate the center point thickness with the blend of Sybil centers and average center points from that case to shield the normal center point from Sybil center point gathering information from various centers checked by edge regard. It overcomes a couple of negative imprints, for instance, takes correspondence time is less, a subset of neighboring information it bears that size of the center point thickness is high(not recognize the Sybil node easily). Be that as it may, occasionally the extent of correspondence makes hard to distinguish the phony node is the most cynical situation. A Sybil attack is recognized when no less than two interesting identities have for all intents and purposes a comparable position. Impediment figuring is used to perceive and check the physical region mapping from different node identities.

2.2.1 RSSI method:

RSSI (Received Signal Strength Indicator) is used for measuring the power level at a different time on the same physical territory. RSSI is time differentiate and deluding nature" communicates that fakes node refinement in radio transmission control. This is a variant endorsement. The issue is to find the incomparable range of the phony (Sybil) node. RSSI handle distinctive observer estimations is to easily recognize the phony node, because of this figuring counterfeit node can't change the radio transmission control. Different gatherer center points have focused on the same center point as sending ID at a different time by figuring the extent of RSSI from heterogeneous center points. It could be figured in different cases according to the distinguishing proof.

2.2.2. TDOA method:

TDOA (Time Difference on Arrival) is focusing on the issues, for instance, correspondence overhead and memory. It is a lightweight game plan. This is a typical endorsement. This framework resembles RSSI however rather than viewing the node from the various recipient, time-based position design is used here. TDOA has based to taken the centroids from a different region and after that perceive the Sybil attack point by figuring the extent for finding most thickly passed on the region and its screw up in the same zone, this range botch has thought to be Sybil node.

2.2.3 CRSD method:

CRSD (Cooperative RSS based Sybil acknowledgment) is used to finish up the detachment between two individual identities by using got signal quality. This supposition has settled transmission power and static framework. This is a quick endorsement. The position could be settled when centers have the same position and partition associations, to be as one social affair with help of RSS. In any case, arrange is a periodical area, the hub accumulates its neighbors and conveys the get-together outcome. The second stage its social occasion result has been gotten and the node can continue running for Sybil attack (question hoard) and what's more, Sybil loosening up (Sybil gather). Like each and every node has been collected with the help of same RSS neighbor center point information's. It guarantees the system execution that reducing the probability of false positive rate and false negative rate.

2.2.3 K-mean method:

K means the technique is RSS based distinguishing proof method. It is used to distinguish the strike according to the movements of transmission power and time assortment. This acknowledgment is an underhanded endorsement. The decision has in light of the status of observation by different center points. In case the discernment has a place with affirmation region it will be recognized, by and large not recognized. This is molded by gathering system. The division is registered by Euclidean detachment between the center point using centroid centers. The examination has on conditions (i.e.) when the impression of center point take a long time and More power, this is believed to be Sybil center, by and large not a Sybil center (take brief time and less power).

3. CONCLUSION

In this paper, a number of existing methodologies for the detection of the Sybil attack have been studied and an algorithm is proposed for detection of Sybil attack in a wireless sensor network. The throughput and packet delivery ratio of the network, before and after detection is analyzed for different traffic rates. It is found that the throughput and packet delivery ratio after detection has improved. At the same time, it judges Sybil attack by using the received signal strength of nodes and the status messages of member nodes which are accumulated in head nodes synthetically. Consequently, aiming at the Sybil attack in head nodes and member nodes, we devise two ways to check and raise the efficiency and refinement of the Sybil attack. On the basis of stressing cluster detection, we put forward the mutual supervision between head node and member node, to detect Sybil attack together. Thus, it improves the accuracy and refinement. The experiment indicates that this method achieves the preferable efficiency wide range practicability, and it is a secure system with self-adaptive detecting capability.

REFERENCES

[1]. J. Newsome, E. Shi, and D. Melody, "The Sybil Attack in Sensor Network: Analysis and Defenses," The Third Intl. Symposium on Information Processing in Sensor Networks (IPSN'04), Berkeley, California, USA: ACN Press, 2004, pp.185-191.

[2]. D. Murat, and S. Youngwhan, "A RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks," World of Wireless, Mobile and Multimedia Networks, WoWMoM 2006. Worldwide Symposium, 2006, pp.259-268.

[3]. J.Wang, G. Yang, Y. Sun, and S.Chen, "Sybil assault recognition in light of RSSI for remote sensor arrange," WiCom '07: International Conference on Wireless Communications, Networking and Mobile Computing, September 2007, pp. 2684-2687, 21-25.

[4]. L. Shaohe, W. F. Xiaodong, Z. Xin, and Z. Xingming, "Identifying the Sybil Attack Cooperatively in Wireless Sensor Networks," in International Conference on Computational Intelligence and Security, CIS '08. Vol.1 2008, pp.442-446.

[5]. Z. Qinghua, W. Skillet, S. Douglas, and P Ning, "Guarding against Sybil assaults in sensor systems," Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshop (ICDCSW'05), 2005, pp.185-191.

[6]. J.R. Douceur. The Sybil assault. In First International Workshop on Peer-to-Peer Systems (IPTPS'02), Mar. 2002.

[7]. Kavitha. P, Keerithana. C "Portable id construct Sybil Attack Detection in light of the Mobile ADHOC Network", International Journal of Communication and Computer Technologies, Volume 2(2014).

[8]. Ayushi "A Symmetric Key Cryptographic Algorithm" International Journal of Computer Applications, Volume 1,No. **15(2010).**

[9]. Abirami.K, Santhi.B "Sybil assault in Wireless Sensor Network" International Journal of Engineering and Technology (IJET)