A Power Efficient Method to Prevent Sybil Attack in Wireless Sensor Network

Reshma Dafade, Prof. Riya Quereshi,
Student, Guide
Computer Science and Engineering
Ballarpur Institute of Technology, Ballarpur,India

***Abstract* - Security is important for many sensor network applications. A particularly harmful attack against sensor and ad hoc networks is known as the Sybil attack , where a node illegitimately claims multiple identities. In a Sybil attack, a malicious user obtains multiple fake identities and pretends to be multiple, distinct nodes in the system. The attacks occur during interactions between the trading peers as a transaction takes place. In this paper we are creating a powerful centralized authority Global Inspector and powers are given to that so that it can identify the Sybil attack by SybilTrust mechanism. The paper based on internal attack in the network. Transmission should be through the GI only. We also show the impact of the attack through an example and simulation results. The algorithm is implemented in Network Simulator.**

***Index Terms* - Wireless Sensor Networks, AODV, Sybil attack.**

1. INTRODUCTION

Wireless Sensor networks are a promising new technology to enable economically viable solutions to a variety of applications, for example pollution sensing, structural integrity monitoring, and traffic monitoring. A large subset of sensor network applications requires security, especially if the sensor network protects or monitors critical infrastructures. Security in sensor networks is complicated by the broadcast nature of the wireless communication and the lack of tamper-resistant hardware (to keep per-node costs low). In addition, sensor nodes have limited storage and computational resources, rendering public key cryptography impractical.

In this paper, we detect the Sybil attack, a particularly harmful attack in sensor networks. In this paper even though if the malicious node is an authenticated node it can be detected as Sybil node. In this paper central authority (Global Inspector) detecting the internal attack in the network. In this paper we are focusing on the result of network having single Global Inspector and multiple Global Inspector. Our work is specially based on security in wireless sensor network and e commerce is the main application of this project. For the security purpose AODV routing protocol is used.

1.1 Motivation

In recent years, wireless sensor network is widely applied in the fields of internet banking, e commerce application etc. It has become the hotspot. Because sensor nodes have limited storage and computational resources, it can easily be assaulted. Various types of attacks such as wormhole attack, sinkhole attack, black hole attack ,selective forward attack, Sybil attack can be present in a network. A particularly harmful attack against sensor networks is the Sybil attack as this attack can make the network easily vulnerable to other attacks. Sybil attack is where a node illegitimately claims multiple identities. Now Sybil attack has caused too much threaten to wireless sensor network in routing, voting system, fair resource allocation, data aggregation and misbehavior detection. Hence many methods are being proposed to detect and prevent Sybil attack in wireless sensor network.

1.2 Abbreviation

GI – Global Inspector

2. SYBIL ATTACK

When a node illegitimately claims multiple identities or claims fake IDs, the WSN suffers from an attack called Sybil attack. The node replicates itself to make many copies to confuse and collapse the network. The system can attack internally or externally. External attacks can be prevented by authentication but not the internal attacks. There should be one to one mapping between identity and entity in WSN. But this attack violates this one-to-one mapping by creating multiple identities [6].

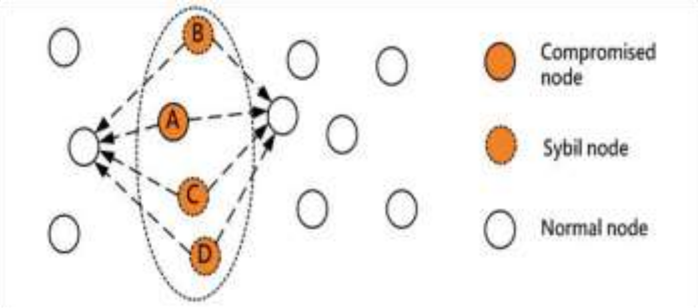

Fig. 1 Sybil Attack

In **Figure 1** A, B, C, D is the Sybil nodes. When these nodes want to communicate to their neighboring nodes they use any one of the identities. This confuses and collapses the network.

3. LITERATURE REVIEW ON SYBIL ATTACK

I. 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 trusted central authority managing the network, and thus knowing deployed nodes. 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 legitimate. Registration is likely to be a good initial defense in many scenarios, with the following drawbacks. 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 add Sybil nodes to the network. In that case there is large communication delay.

II. Position Verification

Another promising approach to defending against the Sybil attack is position verification. Here we 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 generates them. By placing a limit on the density of the network, in-region verification can be used to tightly bind the number of Sybil identities that a malicious node can create.

III. Cryptography

The encryption-decryption techniques devised for the traditional wired networks are not feasible to be applied directly for wireless sensor networks. WSNs consist of tiny sensors which really suffer from the lack of battery power, processing and memory. Any encryption scheme applying on WSNs require transmission of extra bits, hence extra processing, memory and battery power which are very important resources for the sensor’s longevity. Applying the security mechanisms such as encryption could also increase delay, jitter and packet loss in wireless sensor networks [3]. There are some key questions arise when applying encryption schemes to WSNs like, how the keys are generated or disseminated. There is an important issue how the keys could be modified time to time for encryption as there is minimal (or no) interaction for the sensors. There are other many issues how keys are revoked, assigned to a new sensor added to the network or renewed for ensuring robust security for the network. There could not be an efficient solution for adopting of pre-loaded keys or embedded keys.

IV. Challenges in decentralized approaches

Defending against Sybil attacks without a trusted central authority is much harder. Many decentralized systems today try to combat Sybil attacks by binding an identity to an IP address. However, malicious users can readily harvest (steal) IP addresses. Note that these IP addresses may have little similarity to each other, thereby thwarting attempts to filter based on simple characterizations such as common IP prefix. Spammers, for example, are known to harvest a wide variety of IP addresses to hide the source of their messages, by advertising BGP routes for unused blocks of IP addresses [10]. Beyond just IP harvesting, a malicious user can *co-opt* a large number of end-user machines, creating a *botnet* of thousands of compromised machines spread throughout the Internet. Botnets are particularly hard to defend against because nodes in botnets are indeed distributed end users’ computers.

4. PROPOSED DETECTION ALGORITHM

Practically Sybil attack prevention is not that simple. One of the ways of preventing the attack is by having a central authority, such as an administrator who acts as a certifying authority. Administrator can guarantee that each person has a single identity represented by one key. But in practice, this is very difficult to ensure on a large scale and would require costly manual attention. Many algorithms on detecting and defending Sybil attack other than having a central authority have been proposed. In this paper a new method called Global Inspector(GI) has been proposed and combined with SybilTrust is implemented. This approach is expected to give better performance for controlling the Sybil attack. To SybilTrust implementation issue AODV protocol used instead of AOMDV because transaction should be carry out by path detected by GI only.

It includes three phases.

Phase 1 .

- Create a number of wireless nodes in the network.
- One of the nodes is taken as Global inspector or base station.
- The Global Inspector authenticate the node in the network by some criteria
- If the number of nodes in the network is too large then create more than one Global Inspectors.
- The member nodes send their ID and power value to the nearest Global Inspector.

Phase II

- Start transmission between source and destination
- Source node send packet to the Global Insepector
- As soon as source node sending packet to the GI it highlights the destination
- When the transmission between source to GI takes place one of the node in the network pretend as a source then that node is Sybil node.
- The Sybil node is detected by SybilTrust i.e. GI monitoring the routing table of nodes involved in the transmission.
- In that routing table , the GI continuously monitor the IP address of the nodes involved in the transmission.

Phase III

- The routing procedure in the system is used to check the ID of the nodes involved the transmission.
- If the IP address is register but it is not involved during the transmission then that node pretend as Sybil node.
- The routing protocol used in the system is AODV routing protocol.

5. PERFORMANCE EVALUATION

The proposed algorithm is implemented in NS2 and the performance is evaluated in terms of network throughput, packet delivery ratio, and packet drop.

I.Simulation Parameters

The parameters used in our simulation are shown in Table1 A few nodes are selected and given multiple identities which act as Sybil nodes.

Table 1 Simulation Parameters

Area	500mX500m
Nodes	20
Packet size	200bytes
Transmission protocol	UDP
Application Traffic	CBR
Simulation time	100 sec
Queue type	Drop tail
Propagation model	Two Ray Ground
Routing protocol	AODV
Initial energy	100 Joules
Type of attack	Sybil attack

II.Simulation Results

In this section, the performance is analyzed by comparison in between single GI in the group and multiple GI in the group. The result of comparison is analyzed by throughput, energy, delay, and jitter as in **Figure 2**, **Figure 3**, **Figure 4** and **Figure 5** respectively.

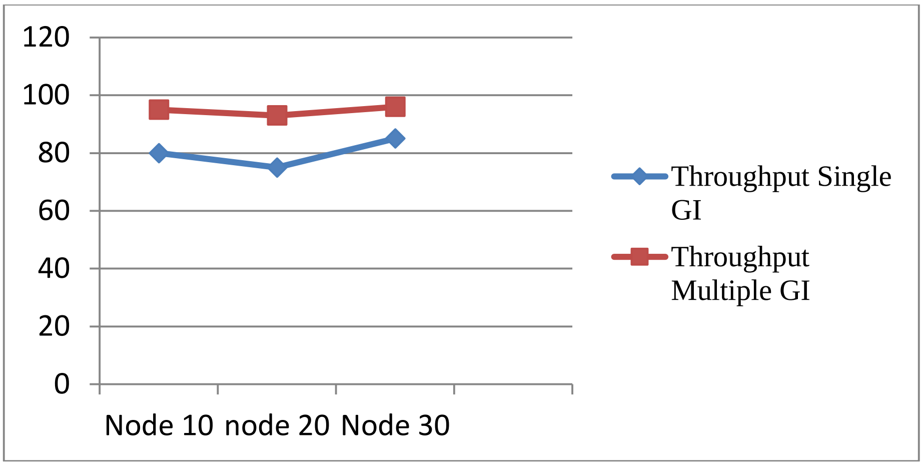

Fig. 2 Comparison of throughput between 10, 20, 30 nodes

As throughput measure the transmission efficiency in terms of successfully delivered packets in unit time for a specified channel bandwidth. The above graph **Figure 2** shows the throughput gain by single GI and comparing it with the multiple GI. The graph interprets that result of multiple GI better than that of single GI. X- axis represents number of nodes and y- axis represents Throughput(MBits/s)

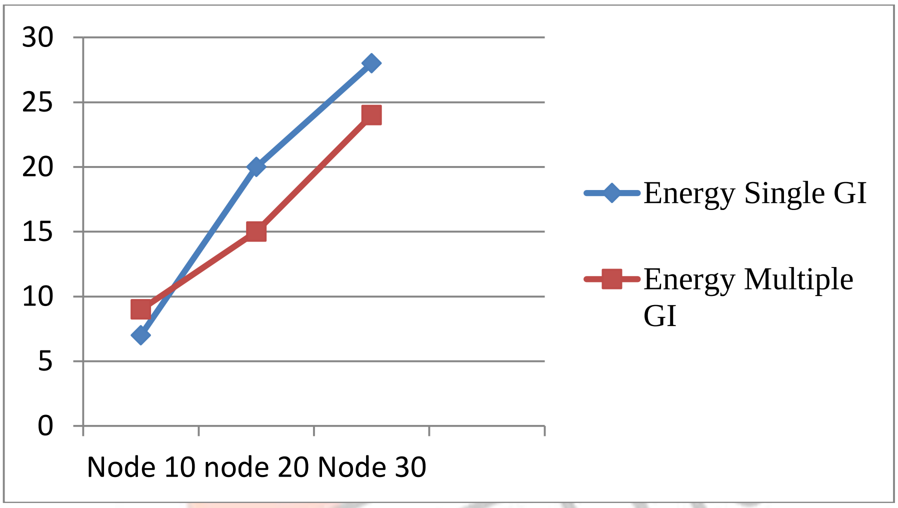

Fig. 3 Comparison of energy between 10,20, 30 nodes

The graph in **Figure 3** shows energy consumption in units for a given wireless sensor network size when the number of nodes are varied within the network. As the nodes increased in the given network energy(energy=power of node* time) consumed will also increases.

X- axis represents number of nodes and y- axis represents energy consumption. In our graph we show that the energy consumption of network having 10 nodes, 20 nodes, 30 nodes. The project graph shows that when there is only one GI in the network then energy consumption is greater than energy consumption when there is multiple GI in the network.

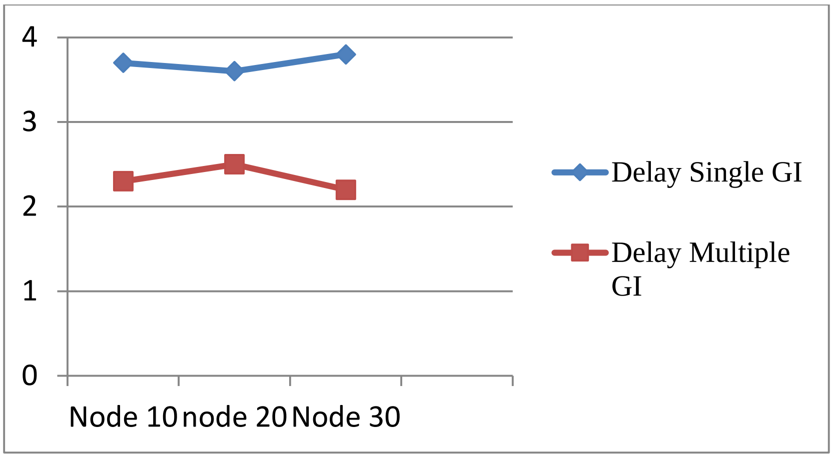

Fig.4 Comparison of delay between 10,20, 30 nodes

The graph in **Figure 4** shows delay of packets by single GI and multiple GI . as shown in the above graph the packet drop rate of single GI is grater than packet drop rate of multiple GI. X- axis represents number of nodes and y- axis represents average end to end delay.

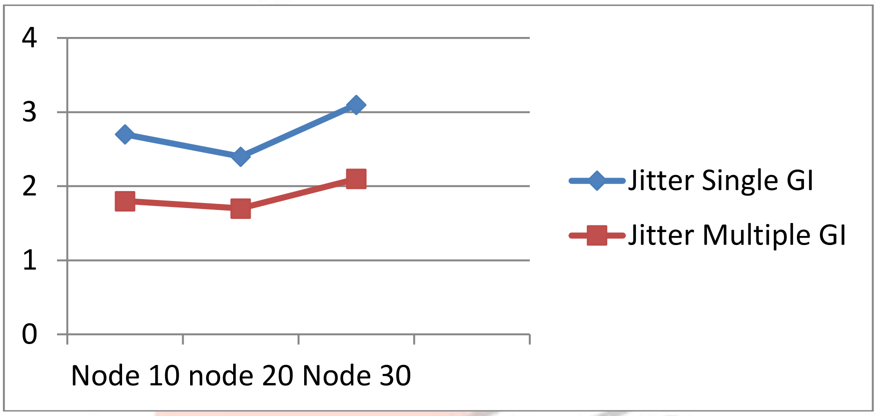

Fig. 5 Comparison of jitter between 10, 20, 30 nodes

As shown in **Figure 5** the jitter rate of single GI is greater than that of multiple GI. Thus form all these graphs we conclude that the network having multiple GI perform so well than single GI.

6. CONCLUSION

A number of existing methodologies for the detection of Sybil attack have been studied and an algorithm is proposed for detection of Sybil attack in wireless sensor network. We are introducing GI(Global Insepector). The throughput and packet delivery ratio of the network, for single GI and after multiple GI. It is found that throughput and packet delivery ratio after multiplication GI has improved.

7. ACKNOWLEDGMENT

This work was based on [1].I would like to thank Department of Computer Science & Engineering, Ballarpur Institute of Technology, Ballarpur for providing infrastructure and guidance to understand Sybil Attack In P2P wireless Sensor Network.

8. REFERENCES

[1] Guojun Wang, Felix Musau, Song Guo, Muhammad Bashir Abdullahi" Neighbor Similarity Trust against Sybil Attack in P2P E-Commerce" in Proc. IEEE Transactiom on Paralle and Distributed Systems, VOL. 26, NO. 3, MARCH 2015.

[2] J. Golbeck, B. Parsia, and J. Hendler, "Trust networks on the semantic web," Cooperative Information Agents VII, pp. 238–249, 2003.

[3] Kumar,P,; Cho,S.;Lee, Y.D.;Lee, H.J.TriSec ," A secure data framework for wireless sensor networks using authenticated encryption,"Int.J.Marit.Inf.Commun.Sci(2010),129-135.

[4] J. Newsome, E. Shi, D. Song, and A. Perrig, “The sybil attack in sensor networks: analysis & defenses,” in Proc. of ACM IPSN, 2004, pp. 259–268.

[5] Natrajan Meghanathan, ―A Location Prediction-Based Reactive Routing Protocol to Minimize the Number of Route Discoveries and Hop Count per Path in Mobile Ad Hoc Networks‖- Department of Computer Science, Jackson State University, Jackson, MS 39217, USA.

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

[7] G. Danezis and P. Mittal, “SybilInfer: Detecting Sybil attack peers using social networks,” in Proc. Netw. Distrib. Syst. Security Symp.San Diego, CA, USA, Feb. 2009, pp. 1–15.

[8] F. Musau, G. Wang, and M. B. Abdullahi, “Group formation with neighbor similarity trust in P2P e-commerce,” in Proc.IEEE Joint Conf. Trust, Security Privacy Comput. Commun., Nov. 2011, pp. 835–840.

[9] H. Rowaihy, W. Enck, P. McDaniel, and T. L. Porta, “Limiting Sybil attacks in structured p2p networks,” in INFOCOM 2007: 26th IEEE International Conference on Computer Communications, 2007.

[10] A. Ramachandran and N. Feamster. Understanding the network-level behavior of spammers. In *ACM SIGCOMM*, 2006

[11] H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao, “SybilLimit: A nearoptimal social network defense against Sybil attack,” IEEE/ACM Trans. Netw., vol. 18, no. 3, pp. 3– 17, Jun. 2010

[12] J. Dinger and H. Hartenstein, “Defending the sybil attack in p2p networks: Taxonomy, challenges, and a proposal for self-registration,”in ARES ’06: Proceedings of the First IEEE International Conference on Availability, Reliability and Security, 2006

[13] N. Tran, B. Min, J. Li, and L. Submaranian, “Sybil-resilient online content voting,” in Proceedings of the 6th Symposium on Networked System Design and Implementation (NSDI), 2009.

[14] H. Yu, M. Kaminsky, P.B. Gibbons, and A. Flaxman, “SybilGuard: Defending against Sybil attack via social networks,” IEEE/ACM Trans. Netw., vol. 16, no. 3, pp. 576 – 589, Jun. 2008.

[15] B.S. Jyothi and D. Janakiram, “SyMon: A practical approach to defend large Structured P2P systems against Sybil attack,” Peer-to-Peer Netw. Appl., vol. 4, pp. 289–308, 2011.

[16] Geetha Jayakumar and Gopinath Ganapathy, ―Performance Comparison of Mobile Ad-hoc Network Routing Protocol‖, International Journal of Computer Science and Network Security (IJCSNS), VOL.7 No.11, pp. 77-84 November2007.