# SYBILSECURE: AN ENERGY EFFICIENT SYBIL ATTACK DETECTION TECHNIQUE IN WIRELESS SENSOR NETWORK

Mr. A. Babu Karuppiah[1], A. Raja Prakash[2]

[1]Assistant Professor,
[2] Final year student,
[1, 2] Velammal College of Engineering and Technology, Madurai, India

***ABSTRACT:***

*A wireless sensor network consists of many sensor nodes which are deployed to monitor physical or environmental conditions and to pass the collected data to a base station. Though wireless sensor network is subjected to have major applications in all the areas, it also has many security threats and attacks. Among all threats such as sinkhole, wormhole, selective forwarding, denial of service and node replication, Sybil attack is a major attack where a single node has multiple identities. When a Sybil node act as a sender, it can send false data to its neighbors. When it acts as receiver, it can receive the data which is originally destined for a legitimate node. The existing solutions consume more energy. So an energy efficient algorithm named Sybilsecure is proposed. Experimental results show that Sybilsecure consumes less energy than existing defense mechanisms.*

***KEYWORDS:***

*Wireless sensor network, Sybil, cluster head, query packet.*

## 1. INTRODUCTION:

Wireless sensor networks consist of as many numbers of nodes which can communicate with each other. Each node consists of a microcontroller, an electronic circuit for interfacing with sensors and battery, a radio transceiver and an external memory. Wireless sensor networks are being used for various applications such as area monitoring, healthcare monitoring and monitoring the combat zone for security purposes. But due to the broadcast nature in wireless communication and low physical protection of sensor nodes, an intruder can easily tend to attack the network. Various attacks on each layer are listed in the table below.

DOI : 10.5121/ijist.2014.4314 

Table 1. Attacks on different layers

| Layer | Attack |
|---|---|
| Physical | Jamming , Node destruction |
| Data link | Denial of service |
| Network | Spoofing, replaying, Hello floods,Homing ,Sybil |
| Transport | SYN flood , De synchronization attack |
| Application | Reprogramming attacks |

In this paper, an efficient algorithm against Sybil attack is proposed as it is a huge destructive attack in sensor networks. In case of Sybil attack, a sensor node behaves as if it were a larger number of nodes, by faking other nodes. Sybilsecure is based on the querying and acknowledging the nodes.

## 2. RELATED WORK:

The existing mechanisms include centralized and decentralized approaches. The vast implemented solution is trusted certification [12],[13]. This solution assumes that there is a special trusted third party or central authority, which can verify the validity of each participant, and further issues a certification for the honest one. In reality, such certification can be a special hardware device or a digital number. Note that essentially both of them are a series of digits, but are stored on different media. Before a participant joins a peer-to-peer system, provides votes, or obtains services from the system, first his identity must be verified. This method gets its limitation when it is applied for larger network. Another method works based on the resource used by the node. If a Sybil node exists then it has to perform the tasks of the identities it possess. So when it exceeds a threshold value then the Sybil node is detected. [14].Secret key [15] can also be shared but it consumes more power as it involves in complex encryption and decryption techniques. In contrast to existing solutions that are based on sharing encryption keys, RSSI based scheme [16] presents a solution for Sybil attack based on received signal strength indicator (RSSI) readings of messages. Though it is said to be lightweight (i.e., only one message communication), it is time-varying, unreliable and radio transmission is non-isotropic. Accuracy reduces as the transmission distance increases. Recent researches in Sybil defense mechanisms are based on Social network based schemes [1] [2] [3] [4] [8] [10] [13] [14]. These schemes use the trust structure embodied in the networks. They have two assumptions, 1) Sybil nodes can create arbitrarily number of identities but relationship to non-Sybil nodes. Sybil nodes are poorly connected to non-Sybil nodes. 2) One trusted non-Sybil node is known. Based on these assumptions various defense schemes such as Sybilguard, Sybillimit, Sybilcontrol , Sybilinfer , Sumup,Gatekeeper are proposed.

## 3. PROPOSED WORK:

The proposed solution is based on sending and responding to the query sent by the cluster head. The Cluster head has a list of its sub nodes parameters. The parameters are the identities and their location.

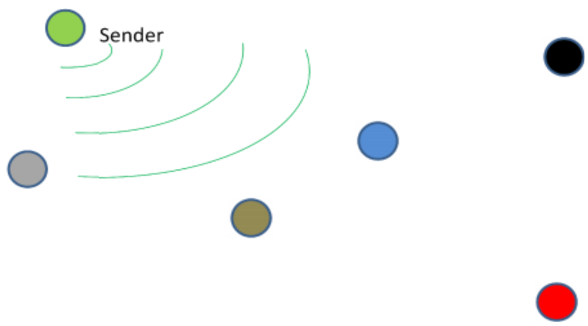


Fig.1. Network with a Cluster head, 4 legitimate nodes and a Sybil node.

Table 2. Dataset in Cluster head

| NODE | DATASET |
|---|---|
| | 1,X<br>2,Y<br>3,Z<br>4,A |

The Cluster head broadcasts a query packet to all the sub nodes in such a way that it expects a reply that all the sub nodes must send their id and location. There are there cases in which the Sybil node reacts.

### (i) No reply:

When a query packet is received by all the legitimate sub nodes including Sybil node, it does not respond to it. It simply gets the packet and drops it. Whenever retransmission is done for multiple times, the Sybil node does not respond to it.

### (ii) Replies with same Identity and different coordinates:

In this case, all the legitimate sub nodes respond to the cluster head with their identity and location. The Sybil node also responds to the cluster head with any one of the Sub nodes identity and its own location. For example, If a cluster head has 4 nodes say 1,2,3,4 with the location x, y, z, a respectively, Sybil node must have any one these identity (1/2/3/4) and its own location d. Now the Sybil node responds with any one of these identities and the location d. The cluster head already has the set of legitimate nodes identity and location. Conflicts arise when the legitimate node and Sybil node has same and different location. The node with the different location is detected as Sybil node.

Table 3. Acknowledgements received

| NODE | ID | LOCATION |
|---|---|---|
| | 1 | X |
| | 2 | Y |
| | 3 | Z |
| | 4 | A |
| | 1/2/3/4 | B |

**(iii) Replies with same identity and same coordinates:**

This case will be future scope of this paper.

## 4. ENERGY CALCULATION:

In wireless sensor network energy consumption is a major factor. Because when a node runs out of battery, it becomes a major problem in network. A dead node will affect entire communication. So the energy consumed by the network to detect a Sybil node is calculated. Based on the formulae from [17], the energy values are calculated. Equations (1) and (2) show the energy for cluster head and a node respectively.

$$E_N(ij) = b\, V_{sup}\, I_{sense}\, T_{sense} + b\, V_{sup}\, (I_{write} T_{write} + I_{read}\, T_{read}) + b\, E_{elec} + B d^{n}_{ij}\, E_{amp} + T_A\, V_{sup}[C_N\, I_A + (1-C_N) I_S] \quad \ldots (1)$$

$$ECH(j) = h_3\, b\, V_{sup}\, I_{sense}\, T_{sense} + h_4\, V_{sup}\, (I_{write} T_{write} + I_{read}\, T_{read}) + h_1\, b_1\, N_{CYC}\, C_{avg}\, V^{2}_{SUP} (n_j+1) + h_1\, b_1\, V_{sup}\, (I_0\, e^{(Vsup/Np\ VT)}\, (N_{CYC}/f)\, (n_j+1)$$

$$+ h_2\, b_1\, E_{elec}\, (n_j) + h_2\, b_2\, (1+\gamma)\, d^{n}_{j}\, E_{amp} + h_2\, \gamma\, b_2\, E_{elec} + T_{CH}\, V_{sup}\, [C_{CH}\, I_A + (1-C_{Ch}) I_S] + E_{actu}\, N_{act} \quad \ldots (2)$$

Consider a network which has a cluster head and four nodes. The tables below show the energy consumed by cluster head and sensor node.

Table 4. Energy consumed by cluster head

| **Cluster head** | **Energy Consumed (J)** |
|---|---|
| Transmit | 0.00784 |
| Transient | 0.049 |
| Sense | 0.594 |
| Data logging | 0.0000385 |
| Receive | 0.00384 |

Table 5. Energy consumed by each node

| **Sensor node** | **Energy consumed** |
|---|---|
| Transmit | 0.00088 |
| Transient | 0.012 |
| Sense | 0.54 |
| Data logging | 0.000035 |
| Receive | 0.00349 |

Upon simulation Sybilsecure takes about 11.327 J to detect a Sybil node. But when considering other social based defense schemes such as Sybilguard and Sybillimit consumes more energy than Sybilsecure. Sybillimit consumes around 8.8 J for a period of time. Sybilguard consumes about 13.48 J for a single round.

# 5. EXPERIMENTAL RESULTS AND COMPARISONS:

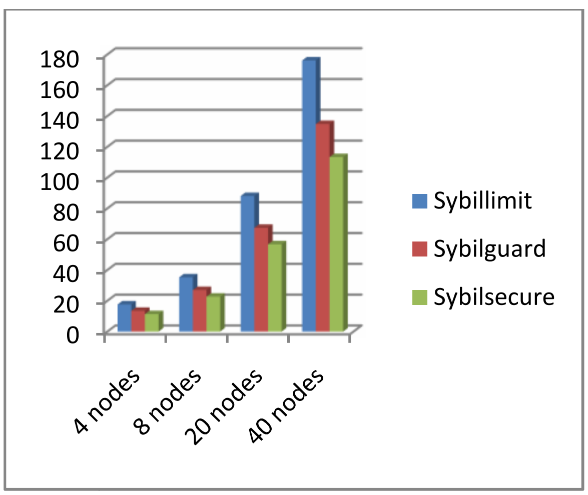


Fig 2.Energy consumed to detect Sybil nodes.

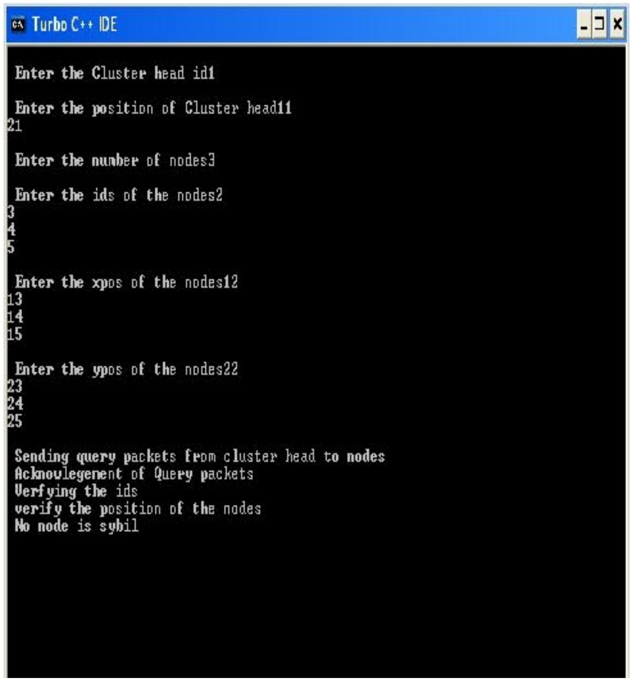


Fig 3. Absence of Sybil node

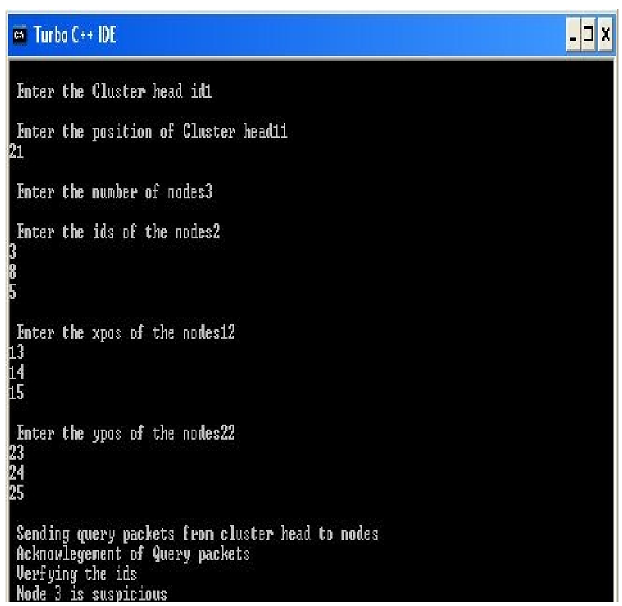


Fig 4. Presence of Sybil node

# 6. CONCLUSION:

In this paper, Sybilsecure,an energy efficient algorithm is proposed based on sending and acknowledging the query data packets. Social network based schemes which involved in random routes of data consumed more energy to detect a Sybil node. But in Sybilsecure , a Sybil node can be detected with less energy and also without decreasing its efficiency.

## REFERENCES:


[1] Bimal Viswanath, Mainack Mondal, Allen Clement, Peter Druschel, Krishna P. Gummadi, Alan Mislove, and Ansley Post, "Exploring the design space of social network-based Sybil defenses", IEEE 2012.

[2] Nguyen Tran, Jinyang Li, Lakshminarayanan Subramanian , Sherman S.M. Chow ,"Optimal Sybil-resilient node admission control ",IEEE, 2009.

[3] Bimal Viswanath, Ansley Post, Krishna P. Gummadi, Alan Mislove, "An Analysis of Social Network-Based Sybil Defenses", SIGCOMM'10.

[4] H. Yu, M. Kaminsky, P. B. Gibbons and A.Flaxman. "Sybilguard: defending against sybil attacks via social networks", SIGCOMM 06.

[5] H. Yu, P. B. Gibbons, M. Kaminsky, and F.Xiao "Sybillimit: A near-optimal social network defense against sybilattacks" In IEEE Symposium on Security and Privacy, 2008.

[6] H. Yu, "Sybil defenses via social networks: a tutorial and survey, ACM SIGACT News, 2011.

[7] G. Danezis, P. Mittal, "SybilInfer: Detecting Sybil nodes using social networks",in Proc. of ISOC NDSS, 2009.

[8] F. Li, P. Mittal, M. Caesar, N. Borisov, "SybilControl: practical Sybil defense with computational puzzles", 7th ACM workshop on Scalable trusted computing, 2012.

[9] C. Lesniewski-Lass, M. F. Kaashoek, "Whanau: A sybil-proof distributed hash table", 7th USENIX Symposium on Network Design and Implementation, 2010.

[10] Wei Wei, Fengyuan Xu, "SybilDefender: A Defense Mechanism for Sybil Attacks in Large Social Networks", Parallel and Distributed Systems, IEEE, 2013.

[11] Nitish Balachandran, Sugata Sanyal,"A Review of Techniques to Mitigate Sybil Attacks", International Journal of Advanced Networking and Applications, 2012.

[12] J. R. Douceur, "The Sybil attack", In Proceedings for the First International Workshop on Peer-to-Peer Systems (IPTPS'02), ser. LNCS, vol. 2429. Cambridge, MA, USA: Springer, Mar. 2002, pp. 251–260.

[13] B. N. Levine, C. Shields, and N. B. Margolin, "A survey of solutions to the Sybil attack", University of Massachusetts Amherst, Amherst, MA, 2006.

[14] J. Newsome, E. Shi, D. Song, and A. Perrig. "The Sybil attack in sensor networks: analysis & defences", In Proceedings of the hird international symposium on Information processing in sensor networks, pages 259–268, 2004.

[15] W. Du, J. Deng, Y. S. Han, and P. K. Varshney," A pairwise key pre-distribution scheme for wireless sensor networks". In ACM CCS 2003, pages 42–51, Oct. 2003

[16] Murat Demirbas, Youngwhan Song, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks, In Proceedings of WoWMoM 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2006. 5 pp. – 570.

[17] M. N. Halgamuge, M. Zukerman, and K. Ramamohanarao, H. L. Vu , "An Estimation Of Sensor Energy Consumption", Progress In Electromagnetics Research B, Vol. 12, 259–295, 2009.