IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 6, June 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

# Implementation of Optimized LEACH Routing Protocol for Detection and Prevention of Sybil Attack in Wireless Sensor Network using BFS

**Deepak Pandey[1], Archana[2] and Poonam Rani[3]**

[1] M.Tech, Computer Science & Engineering, P M College of Engineering, Sonepat-131001, Haryana, India
[2] Assistant Professor and HOD, Computer Science & Engineering, P M College of Engineering, Sonepat-131001, Haryana, India
[3]Assistant Professor in Computer Science & Engineering, NSIT, Delhi, India

**Abstract**

A wireless sensor network (WSN) is an independent network which consists of autonomous sensors which are spatially distributed and used to monitor physical or environmental conditions. Wireless sensor networks have been widely used in emergency operations, military scenarios and natural disaster hit areas. The communication among sensors is via wireless links. This infrastructure less nature of WSN makes it vulnerable to various security attacks. There is an attack which causes many serious threats to the network and it is known as **Sybil Attack**. In Sybil attack, attackers or malicious nodes uses many identities to gain control over the network and creates lots of misconception among nodes. They forge identity of some trustworthy node present in the network and misbehave which leads to large drop of data packets. It also disturbs the communication among the nodes present in the network. In this paper we have implemented the LEACH routing protocol to detect and prevent Sybil attack in WSN. Detection is done by distance and hop count between the nodes and for prevention of Sybil attack we have used encryption technique using Breadth First Search (BFS) Algorithm. Simulation tool used for the implementation is NS2.

**Keywords**: LEACH Protocol, Wireless Sensor Network, Sybil Attack, Sensor Nodes, Encryption, Energy Consumption, Breadth First Search (BFS).

## 1. Introduction

Wireless Sensor Network (WSN) is a special kind of non infrastructure network capable of wireless communication having large number of low-cost sensor nodes which are spatially distributed and used to monitor physical or environmental conditions with limited power and multi-functional capability. A typical sensor node includes four basic components: a sensing unit, a processing unit, a communication unit, and a power unit [7].

WSN is becoming increasingly popular due to the variety of applications. It is widely used in the field of military, education, medical treatment, traffic etc [5]. Peer-to-peer communication exists between nodes of a WSN. Multi-hopping can cause sensor node to communicate with a node that is not in radio range of each other via intermediate nodes. So WSN provides flexibility of adding or removing nodes in the network. The network can be divided into no. of clusters called clustering. In each cluster, one of the sensor nodes is elected as Cluster Head (CH) and the rest of the nodes act as Cluster Members (CM). All sensor nodes work in cooperation within each cluster to serve the request. Cluster head collects the data from its members and data aggregation is done by each cluster head to remove data redundancy and forwarded to the sink. As cluster head consumes more energy than cluster members, the workload of cluster heads is distributed among all nodes in wireless sensor network by rotating their roles to equalize energy consumption.

Energy consumption is an important issue in WSN because sensor nodes are battery operated [1]. The open nature of the wireless communication channel, the lack of infrastructure makes WSN prone to various security attacks. One of the attacks in Wireless sensors network is Sybil attack. In Sybil attack the attacker subverts the wireless sensor network by creating a large number of pseudonymous identities. Sybil attack is defined as a process in which one node copies other node identity and misbehaves in the network.

In this paper, we review the performance of throughput and energy consumption aware Leach against Sybil attack and its prevention using encryption technique with the help of Power, UID and threshold values using BFS

## 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 be attacked 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 [2]. WSN can easily be attacked by Sybil attack as the communication medium of WSN is to broadcast and same energy is shared among nodes.

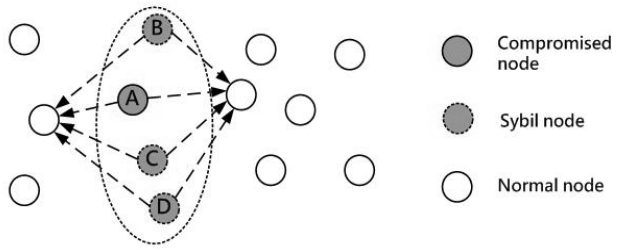


Fig1. Sybil attack on network

Sybil attack is classified into following ways:

**2.1 Direct vs. Indirect communication:**
In direct communication Sybil nodes communicate directly with the legitimate nodes of network while in indirect communication legal nodes are not able to communicate directly with the Sybil nodes. Instead, one or more of the malicious devices claims to be able to reach the Sybil nodes.

**2.2 Fabricated vs. Stolen identities:**
In former case attacker generates random new identities and in latter case the attacker steal an identity from the legal node.

**2.3Simultaneous vs. Non-Simultaneous communication:**
In Simultaneous communication the attacker may try to have his Sybil identities all participate in the network at once. Alternately, in Non-Simultaneous the attacker might present a large number of identities over a period of time, while only acting as a smaller number of identities at any given time.

## 3. LEACH Routing Protocol

Low-Energy Adaptive Clustering Hierarchy (LEACH) [17] is a TDMA-based MAC protocol and a typical hierarchical clustering routing protocol. This clustering hierarchy helps in fragmenting the network into small region called clusters. Each cluster consists of group of nodes and a cluster head (CH).It is the responsibility of cluster head to aggregate and transfer the data collected from the sensor node of a cluster to the base station. In order to optimize energy in the network, nodes are selected as cluster head circularly and randomly. The goal of LEACH is to lower the energy consumption required to create and maintain clusters in order to improve the life time of a wireless sensor network.

The process of formation of clusters in LEACH is shown in figure 2.

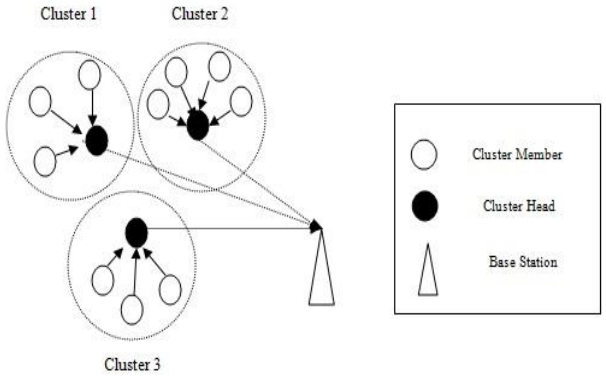


Fig2. Formation of Clusters in LEACH

The LEACH protocol operates in rounds and each round consists of two phases: setup phase and steady phase.

i. **Setup phase:** In the setup phase, the cluster head is elected. The sensor nodes elect a cluster head based on the Threshold equation T (n) [18]:

**T (n) = p/1-p*(r mod 1/p)  if n ∈ G**
**T (n) = 0  otherwise**

Where p is the desired percentage to become a cluster head, r is the current round and G is the set of nodes that have not become the cluster head in the last 1/p rounds. Each node chooses a random number between 0 and 1.If this random number is less than threshold value T (n) then the node becomes the cluster head for the current round.

ii. **Steady state phase** –In the steady state phase the cluster head collects the data from the nodes using TDMA schedule and after aggregating and processing the data transfer it to the base-station [18].

## 4 Proposed Scheme

The individual sensor nodes are anonymous and communication among sensors is via wireless links, therefore sensor networks are highly vulnerable to security risks and attacks that leads to usage of more memory and overhead in the gateways as well as nodes. The basic mechanism used to secure the system from these attacks is the proposed routing protocol 'LEACH'.

Wireless sensor network lifetime is the function of energy. Therefore, consumption of energy is the major issue. Consumption of energy in a network takes place during transfer of data between nodes and distance between the nodes. Sybil attack is the most effective attack on wireless sensor network. Sybil attack forge identity of one of the nodes and misbehaves which leads to large drop of data packets. Prevention mechanism for the Sybil attack will use key distribution technique.

In this section we will introduce a unique and good Sybil attack prevention mechanism for sensor network. Therefore, in order to overcome these stated limitations we are using a proposed new scheme and protocol which will be helpful in scalability and connectivity of the networks in wireless sensor network. Both detection and prevention is done using LEACH routing protocol. The concept of LEACH involves the cluster formation of nodes which leads to minimum energy consumption and less packet drop during the process. Pre-Shared Encryption technique is applied to prevent Sybil attack on WSN. It is done by having three values as Power, UID and Threshold values using BFS. Then the routing procedure in the cluster is checked to verify if there was a hop between the Sybil identities. If there is any hop between the Sybil identities, then the nodes are not Sybil nodes. If there is no hop, the nodes are confirmed to be under attack and they will be removed from the network.

### 4.1 Methodology of detection and prevention of Sybil attack

The figure 3.1 the represents the steps for detection and prevention of Sybil attack in wireless sensor network.

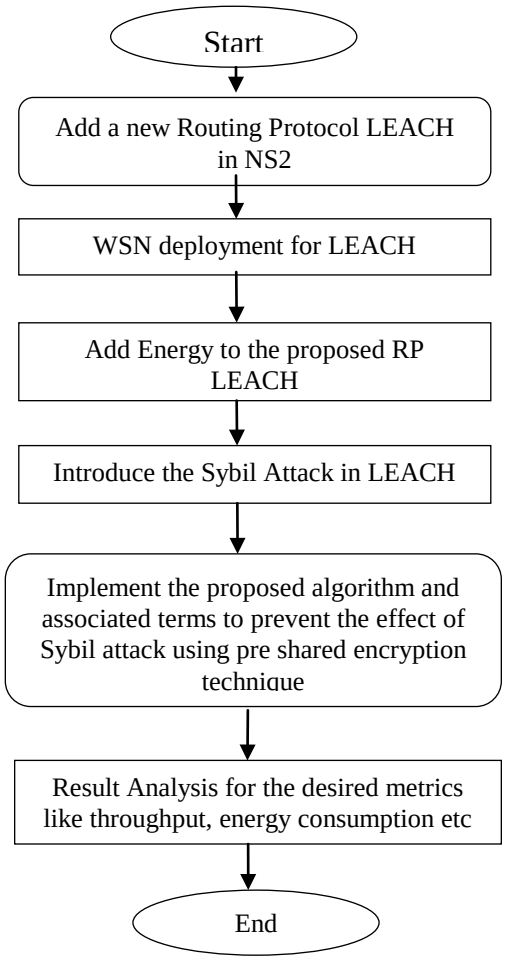


Fig3. Flowchart of Methodology

**Breadth first search** is an algorithm for traversing or searching tree or graph data structures. It starts at the tree root (or some arbitrary node of a graph, sometimes referred to as a search key) and explores the neighbor nodes first, before moving to the next level neighbors. It is used to find the optimized path.

BFS was invented in the late 1950s by E. F. Moore, who used it to find the shortest path out of a maze, and discovered independently by C. Y. Lee as a wire routing algorithm.

A non-recursive implementation of breadth-first search:

```
1 Breadth-First-Search (Graph, root):
2
3   for each node n in Graph:
4       n. distance = INFINITY
5       n. parent = NIL
6
7   create empty queue Q
8
9   root. Distance = 0
10   Q. en-queue (root)
11
12   while Q is not empty:
13
14       current = Q. de-queue ()
15
16       for each node n that is adjacent to current:
17           if n. distance = INFINITY:
18               n. distance = current. Distance + 1
19               n. parent = current
20               Q. en-queue (n)
```

## 5 Simulations and Results

The proposed work is implemented in NS-2 simulations.NS-2 is an event-driven tool useful in studying the dynamic nature of computer network. NS is an object oriented simulator, written in C++, with an OTCL interpreter as a frontend.

After simulating the program using cbr and scenario files we can get the output in form of two files. One is called as the network animator file (NAM) and the other is called the trace file. These two files are created in the due course of running the program. Basically the two files stores the same things but in different format. NAM file stores the output in such a way that it can be used by the animator to show an animated result, and the trace file stores the output so that it can be analyzed.

**Table 1: Simulator Parameters**

| | |
|---|---|
| **Simulator** | **NS2** |
| **Simulation Duration** | **300 sec** |
| **Number of nodes** | **17, 32, 48 and 64** |
| **Traffic Type** | **FTP(TCP)** |
| **Routing Protocol** | **LEACH** |
| **Channel Type** | **Wireless Channel** |
| **Network Interface Type** | **Wireless PhyIEEE 802.11** |
| **Topology** | **1500 X 1150 units** |

In present work performance analysis is done using only single parameter i.e., energy consumption with time having 4 clusters whereas in this proposed work the analysis is done on two parameters which are throughput and energy consumption and their comparison with different number of nodes i.e., 17, 32, 48 and 64 nodes.

The goal of this project is to compare the performance of the two protocols under different scenario. Comparing the different methods is done by simulating them and examining their behaviour. In comparing the two protocols, the evaluation could be done in the following:

**5.1 The throughput** defined as the number of received data packets for different number of nodes. A comparison is done with different number of nodes as shown in fig 4.

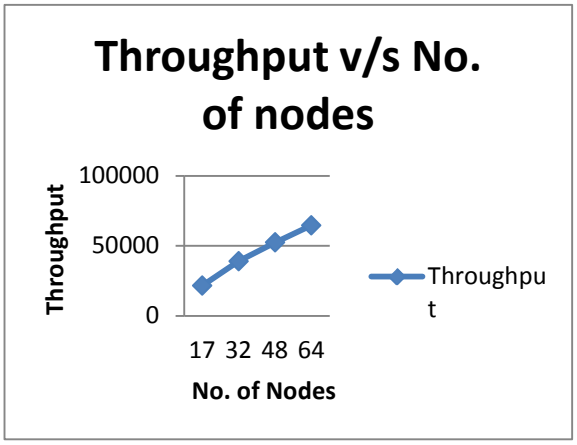


Fig4. Result of Throughput

Values of Throughput analyzed vs. different number of nodes:

- In 17 nodes – **21628** bits per second.
- In 32 nodes – **39061** bits per second.
- In 48 nodes – **52390** bits per second.
- In 64 nodes – **64677** bits per second.

**5.2 The energy consumption** is defined as the amount of energy consumed during the transmission of messages between nodes and cluster head as well as between the cluster head and the base station. Minimum is the consumption maximum is the network lifetime. It is measured in joules.

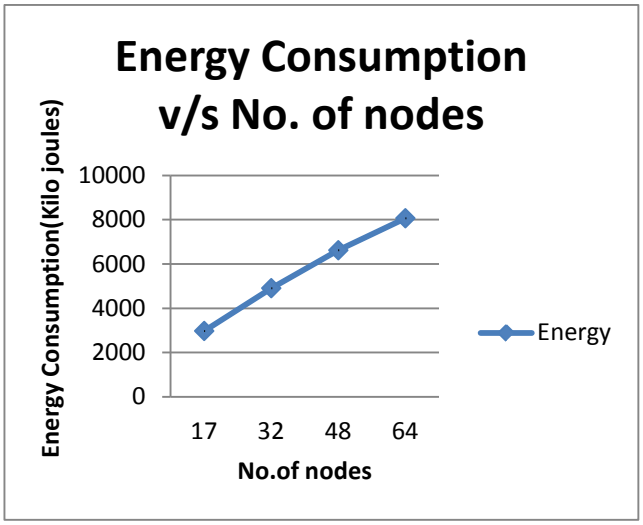


Fig5 Result of Energy Consumption

Values of Energy Consumption analyzed vs. different number of nodes:

- In 17 nodes – **2977380** joules.
- In 32 nodes – **4909540** joules.
- In 48 nodes – **6622620** joules.
- In 64 nodes – **8067580** joules.

## 6 Conclusion and Future Scope

### 6.1 Conclusion

The paper proposed the implementation of efficient routing LEACH protocol to detect and prevent Sybil Attack in wireless sensor network. Wireless sensor network can pose a security attack due to hostile distributed environment and fast implementation practices. The proposed work prevents the wireless sensor network from the security risk that is due to Sybil attack by using the pre-shared encryption technique based on three values which are Power, UID and Threshold value using Breadth First Search (BFS) Algorithm. After prevention of Sybil Attack results like Throughput and Energy Consumption in different clusters having 17, 32, 48 and 64 nodes has been calculated and compared. Simulation has been taken place in NS2 environment.

### 6.2 Future Scope

The work proposed here includes detection and prevention of Sybil Attack. In future it can be improved with the following aspects:

- In future detection and prevention of more attacks can be done.
- In future we can perform this test on a large scale wireless sensor network.
- Also we can test the performance in terms of other metrices other than throughput and energy consumption.\
- We can extend our protocol to tolerate existing Sybil nodes in the network.

## Acknowledgement

I would like to place on record my deep sense of gratitude to my supervisor, **Ms. Archana (HOD-CSE)**, Computer Science and Engineering department, PMCE, Sonepat (Haryana), India for her stimulating guidance, continuous encouragement and timely suggestions during the entire duration of my project work, without which this work would not have been possible and for giving me the freedom to pursue topic of my own interest and providing me with exactly the amount of structure needed to ensure of my success. You have not simply taught me how to succeed as a student, but rather how to be an independent researcher. Thank you so much for all of the academic, professional and personal advice that you have bestowed on me. I would also like to convey my deep regards to all other faculty members and staff of Department of Computer Science and Engineering.
The completion of this dissertation would not have been possible without the boundless encouragement and support of my family. My parents have spent their lives encouraging my intellectual and personal growth. From you all, I have learned to take pride in my work and to enjoy the simple pleasure of a job well done. Thank you for everything that you have given me.

## References


1. H.Chan and Perrig, "*Security and Privacy in Sensor Networks*" IEEE Computer, Vol. 36(10), October 2003, pp. 103-105.
2. 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.
3. J. Newsome, E. Shi, and D. Song, "The Sybil Attack in Sensor Network: Analysis & Defences," *The Third Intl. Symposium on Information Processing in Sensor Networks* (IPSN'04), Berkeley, California, USA: ACN Press, 2004, pp.185-191.
4. Murat Demirbas and 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.
5. S.Sharmila1, G Umamaheswari2 "Detection of Sybil Attack in Mobile Wireless Sensor Networks" [IJESAT], Volume-2, Issue-2, 256 – 262.
6. S. Abbas, M. Merabti, and D .Llewellyn-Jones. Signal Strength Based Sybil Attack Detection in Wireless Ad hoc Networks. *Second International Conference on Developments in e Systems Engineering*, 2009.
7. M. Dhatchayani , *International Journal of Computer Science Trends and Technology* (IJCST) – Volume 2 Issue 1, Jan-Feb 2014.
8. J.Wang, G. Yang, Y. Sun, and S.Chen, "Sybil attack detection based on RSSI for wireless sensor network," WiCom '07: *International Conference on Wireless Communications, Networking and Mobile Computing, September 2007*, pp. 2684-2687, 21-25.
9. L. Shaohe, W. F. Xiaodong, Z. Xin, and Z. Xingming, "Detecting the Sybil Attack Cooperatively in Wireless sensor Networks," *In International Conference on Computational Intelligence and Security*, CIS '08. Vol.1 2008, pp.442-446.
10. B. N. Levine, C. Shields, and N. B. Margolin, A survey of solutions to the Sybil attack, University of Massachusetts, Amherst, MA, 2006.
11. P.W. L. Fong. Preventing Sybil Attacks by Privilege Attenuation: A Design Principle for Social Network Systems. In *IEEE Symposium on Security & Privacy*, 2011 pp. 263-278
12. Diogo Monica, Thwarting the Sybil Attack in Wireless Ad Hoc Networks, Master's Thesis at the Universidade Tecninca de Lisboa, July 2009.
13. Z. Qinghua, W. Pan, S. Douglas, and P Ning, "Defending against Sybil attacks in sensor networks," *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshop* (ICDCSW'05), 2005, pp.185-191.
14. S.Lv, X.Wang,X.Zhao and X.Zhou, Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks, IEEE, pp 442-446, 2008.
15. X.Li, Han, A.Qian, L.Shu and J.Rodrigues "Detecting Sybil Attack based on State Information in Underwater Wireless Sensor Networks," IEEE, 2013.
16. Tahir, H., Shah, S., "Wireless Sensor Networks – A Security Perspective" *12th IEEE International Multi topic Conference*, December 23-24, 2008 (pp.189-193).
17. Heinzelman, W. Rabiner, A. Chandrakasan, and H. Balakrishnan. "Energy-efficient communication protocol for wireless microsensor networks." *In System sciences, 2000.*
18. S. Lee, Y. Lee and S.G. Yoo, "A Specification Based Intrusion Detection Mechanism for the LEACH Protocol, Information Technology Journal," pp 40-48, 2012.