Optimized secure routing protocol to prevent Sybil attack in wireless sensor networks

Prameet Kaur and Dr. Sandeep Singh Kang

Abstract— A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. WSN's are a latest type of networked systems, characterized by strictly limited computational and energy resources, and an ad hoc operational environment. Wireless sensor networks have been widely used in emergency operations, habitat monitoring, remote areas, military scenarios, sensing motion applications, agriculture solutions and natural disaster hitted areas. For explicit application, it requires strong authentication and security mechanism for more security. Wireless sensor network are easy vulnerable to attack one of which is Sybil attack. Sybil attack is harmful against routing protocol which can drop data randomly. Sybil attack is defined as a process in which one node copies other node identity and misbehaves in the network. In this paper, we propose a security based on LEACH routing protocol against Sybil attack. LEACH (Low Energy Adaptive Hierarchy) routing protocol is the conventional clustering communication protocol which is commonly used in Wireless Sensor Networks. Major issue with LEACH routing protocol is energy consumption. In order to balance the energy consumption of each node, the nodes are selected as cluster head randomly and circularly. The mechanism is set up to detect Sybil attack based on the distance and hop count between the nodes and the prevention is done using encryption technique which is based on unique identities of the nodes. The performance parameters energy consumption is calculated. Its values show the efficiency of the proposed protocol.

Index Terms— Encryption, energy consumption , LEACH protocol, Malicious node, Wireless sensor network, Sybil attack, Sensor Nodes

1 INTRODUCTION

Wireless network consist large number of sensor nodes which communicate with each other using wireless links. Sensor nodes collect data from their surrounding environment and send this sensed data to the sink node. WSN have characteristics that are unique to them, such as the ability to withstand unfavorable environmental conditions, dynamic network topology, communication failures, large scale of deployment, scalable node capacity, node mobility, unattended operation as well as limited power, to name a few. WSN consist of base stations, which have more resources such as more energy that act as a gateway between the sensor nodes and the end user. The energy source of sensor nodes in wireless sensor networks (WSN) is usually powered by battery, which is not likely, even impossible to be recharged or replaced. Therefore, improving the energy efficiency and minimizing the message overhead are the major challenges in sensor networks. Wireless sensor networks (WSNs) are playing a promising role in a variety of application areas, such as military, home applications and environment monitoring.

- *Prameet Kaur is currently pursuing masters degree program in computer science engineering from CGC, Landran, PTU, India, E-mail: prameet.it@gmail.com*
- *Dr. Sandeep Singh Kang is working at CGC-COE, Landran as HOD (CSE) , India, E-mail: sskang4u1@rediffmail.com*

For example, in emergency response operations such as after a natural disaster like a flood, tornado, hurricane, or earthquake, sensor networks could be used for real-time safety feedback, regular communication networks may be damaged, so emergency rescue teams might rely upon sensor networks for communication.

The open nature of the wireless communication channel, the lack of infrastructure, the fast implementation practices and the hostile distributed environments, make WSN prone to various security attacks. The attacks can be active and passive attacks. A passive attack attempts to make use of the information of the network but does not affect the normal functionality of a network. A passive attack can be capturing data without altering it. The active attacks attempts to alter network and even affect their operation. The active attacks are classified as external and internal attacks. An attack from within the network is an internal attack whereas an attack from a foreign network is an external attack.

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, using them to gain a disproportionately large influence.
In this paper, we reviews the performance of energy aware Leach against Sybil attack and its prevention using encryption

scheme following requisite functions for every terminal end. The rest of the paper is organized as follows: Section II describes the Sybil attack, Section III discusses the LEACH protocol , Section IV presents proposed scheme, Section V contains simulations and results and in Section VI conclusions.

2 Sybil Attack

Sybil attack is a type of attack in which the attacker (Sybil node) tries to forge multiple identification in certain region. WSN can easily be attacked Sybil attack as the communication medium of WSN is to broadcast and same energy is shared among nodes. By broadcasting messages with multiples identification, a Sybil node can manipulate the vote on group based decisions and also disrupt network services.

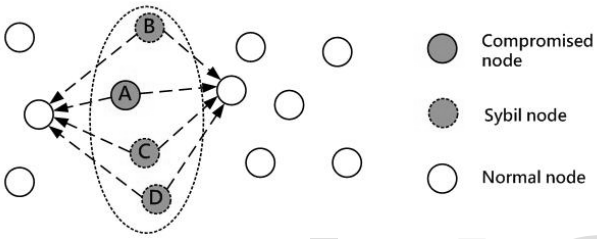

Fig 1. Sybil attack on network

Sybil attack is classified into following ways:

1. Direct vs. Indirect communication:
   In direct communication Sybil nodes communicate directly with the legitimate nodes of network. When a genuine node sends a message to a Sybil node, one of the malicious devices listens to the message while in indirect communication legal nodes are not able to communicate directly with the Sybil nodes rather than one or more of the malicious devices may state to be able to reach the Sybil nodes.
2. Fabricated vs. Stolen identities
   In former case attacker generate random new identities and in latter case the attacker stole an identity from the legal node.

3 LEACH Routing Protocol

Low Energy Adaptive Clustering Hierarchy ("LEACH") is a TDMA-based MAC protocol which is integrated with clustering and a simple routing protocol in wireless sensor networks (WSNs). 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 operation of LEACH is split into rounds and each round is divided into two phases namely as: setup and steady-state phase. Steady-state phase is always long compared to the set-up phase to minimize the overhead. In LEACH protocol, the SNs arrange themselves into local clusters, with one node acting as the leader which defined as cluster head (CH) and rest of the nodes act as ordinary nodes which are remembers of the cluster head. To prolong the lifetime of the network, LEACH includes randomized rotation of the high-energy CH and performs local data fusion to transmit the amount of data being sent from the CHs to the BS. If BS is far away from the network then the energy of CHs will be affected as only CHs are directly communicating with the BS. Set of clusters will be different for different time interval and the decision to become a CH depends on the amount of energy left at the SN.

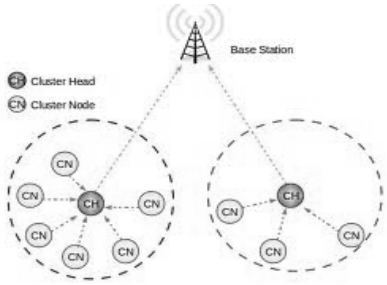

Fig 2. Network model

The decision is made by selecting the node n choosing a random number between 0 and 1. If this is less then threshold $T(n)$,the node becomes cluster-head for the current round. The threshold level is set by:

$$T(n) = \frac{p}{1-p*(r \bmod (1/p))} \quad \text{if } n \in G$$
$$= 0 \quad \text{otherwise}$$

Where the p = desired percentage of cluster heads
r = the current round
G is the set of the nodes that have not been cluster-heads in the last rounds.

4 Proposed Scheme for Sybil Attack Detection and Prevention

In this section, we will describe the process to detect and prevent Sybil attack in WSN. We start the procedure by adding the security routing LEACH protocol in wireless sensor network. Now, create a group of mobile nodes. One of the nodes is selected as base station. Base station sends HELLO packets to all the node of the network. Nodes with the minimum packet drop are selected as trust node. The elected node becomes the head node with the group of member nodes. The member nodes send their ID and power value to the head nodes. The head node checks for nodes with the power value less than threshold value. If the situation is true then the node is detected as Sybil node. Detection of Sybil attack is based on the distance between the nodes and hop count between them.

Encryption technique is applied to prevent Sybil attack on WSN's. It is done by distributing the unique identities to each node of the cluster. Then the routing procedure in the cluster is checked to verify if there was a hop between the Sybil identities. It takes place in following ways:

1. If there exists a 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.
2. In the next phase two nodes closer to Sybil nodes are selected as sender's s1 and s2. The hop between the Sybil nodes and Sybil identities are analyzed. If the hop exists then the nodes are not Sybil nodes.

Both the detection and prevention scheme is implemented using all the requisite data as per simulation necessity and key which have to be implemented on basis of binomial distribution.
The binomial distribution is the discrete probability distribution of the number of successes in a sequence of n independent yes/no experiments, each of which yields success with probability p. If the random variable X follows the binomial distribution with parameters n and p, we write $X \sim B(n, p)$. The probability of getting exactly k successes in n trials is given by the probability mass function:

$$f(k;n,p) = \Pr(X = k) = \binom{n}{k} p^k (1-p)^{n-k}$$
for k = 0,1,2...., n where
$$\binom{n}{k} = n!/k!\,(n-k)!$$

is the binomial coefficient, hence the name of the distribution. The formula can be understood as follows: we want k successes (p^k) and $n - k$ failures $(1 - p)^{n-k}$.

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.

Table 1: Simulator Parameters

Parameter	Values
Simulator	NS-2
Simulation Duration	450 sec
Topology	2500meter X 2500 meter
No. Of nodes	104
Maximum segment size	512
Traffic type	FTP (TCP)
Routing protocol	LEACH
Channel Type	Wireless Channel
Network Interface Type	Wireless PhyIEEE 802.11

The whole process consists of total of 104 nodes divided into 4 clusters each containing 25 nodes each and consists of one base station with each cluster. Each cluster has one head node which communicates to the base station to transmit data. The proposed scheme detects the Sybil attack in the wireless sensor using efficient routing protocol. The performance analysis of the proposed work is presented using parameter these are energy consumption.

Energy consumption: Energy consumption is defined as the consumption of energy or power. It is the amount of energy consumed during the transmission of message between nodes and cluster head and nodes of the cluster and transmission between the cluster head and the base station. Fig shows the impact of Sybil attack on the network.

Minimum is the consumption of energy while transmission maximum is the network lifetime. Variation in the value is due to the impact of Sybil attack due to which packet drop takes place and sometimes it reaches to zero also. It is measured in joules.

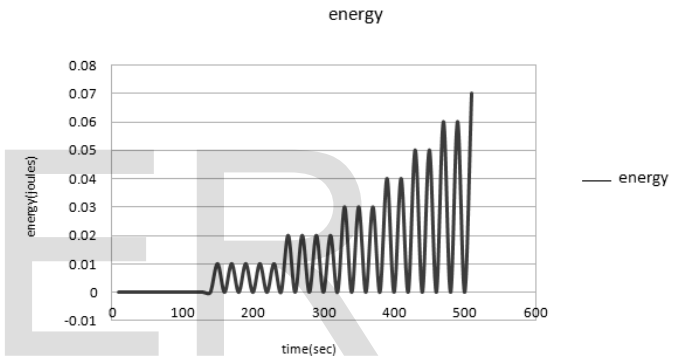

Fig 3. Impact of Sybil attack on the network

6 Conclusion

The paper proposed the efficient routing LEACH protocol to 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 encryption technique based on the binomial distribution. In future more attacks can be simulated and can check the performance of the proposed work.

Acknowledgement

I express my sincere gratitude to the Punjab Technical University, Jalandhar for giving me the opportunity to work on the thesis during my final year of M.Tech.
First of all I am thankful to my project guide Dr. Sandeep Singh Kang, HOD, Computer Science and Engineering Department, CGC College of engg, Landran under whose guideline I was able to complete my thesis. I am wholeheartedly thankful to him for

giving us their valuable time and attention and for providing us a systematic way for completing my project.
I must make special thanks of faculty members for their co-operation and assistance in solving problems. I would like to thank our Head of department, Mr. Rajwinder Singh, Computer Science and Engineering Department and all assistants for providing us assistance in various hardware and software problem encountered during course of our project.
Thesis work is an important aspect in the field of engineering. I would also like to thank my parents, friends etc who helped me in my thesis.
I would also like to thank everyone who has knowingly & unknowingly helped me throughout my thesis. Last but not least, a word of thanks for the authors of all those books and papers which I have consulted during my thesis work as well as for preparing the report.

REFERENCES

[1] Tahir, H., Shah, S., "Wireless Sensor Networks – A Security Perspective" 12th IEEE International Multitopic Conference, December 23-24, 2008 (pp.189-193).

[2] Xie, M., Han, S., Tian, B., Parvin, S., "Anomaly Detection in Wireless Sensor Networks: A Survey" Journal of Network and Computer Applications 34 2011(pp.1302–1325).

[3]Burgner, D., Wahsheh, L., "Security of Wireless Sensor Networks" Eighth International Conference on Information Technology: New Generations2011(pp.315-320).

[4]Yanjing, S., Yanjun, H., Beibei Z., Xue, L., "An energy efficiency clustering routing protocol for WSNs in confined area" ,Sciencedirect Mining Science and Technology (China) 21, 2011 (pp.845–850).

[5]Wang, S., Yan,K., Wang, S., Liu, C., "An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks", ScienceDirect Expert Systems with Applications 38,2011 (pp.15234–15243).

[6] Jianyin, L., "Simulation of Improved Routing Protocols LEACH of Wireless Sensor Network" 7th International Conference on Computer Science & Education (ICCSE 2012) July 14-17, 2012. Melbourne, Australia, (pp.662-666).

[7]Lu, Y., Zhang, D., Chen, Y., Liu, X., and Zong, P., "Improvement of LEACH in Wireless Sensor based on Balanced Energy Strategy" IEEE International Conference on Information and Automation Shenyang, China, June,2012 (pp.111-115).

[8] Jun, L., Hua, Q., Yan, L., "Modified LEACH algorithm In Wireless Sensor Network Based on NS2" International Conference on Computer Science and Information Processing (CSIP), 2012 (pp.604-606).