# SECURITY IS THE PRIMARY GOAL FOR DESIGNING A WSN

AvikModak
DepertmentOf ECE
MCKV Institute Of Engineering
avikmodak@ymail.com

Anuran Roy Chowdhury
Depertment Of ECE
MCKV Institute Of Engineering
anuranforu@gmail.com

***Abstract*: We are aware thatthe power limitation is a critical issue for the sensor nodes, so different scheme or algorithm was proposed to implement the routing protocols to expand the minimum power utilize the maximum work [1,2].But it is unfortunate that most of them are not security concerned. As we know that the wsn is used for military purpose mainly so fulfilling privacy and security requirements in an appropriate architecture for WSNs offering pervasive services is essential for acceptance. Though prolonged lifetime may help the sensor network to work for several yearwithout change the battery of the nodes but still it is the security that is most needed. If an attacker may hack the information of the network then prolonged lifetime have no importance to the network as longer the lifetime of the network more information will be hacked. In this paper we will discuss some internal and external security aspects that the routing protocols have faced and different solutions to make the protocols secure as well as prolonged life time concerns.**

***KeyWords:*SecureRouting,Lifetime,Attacks, Privacy, Cryptography.**

## *I. INTRODUCTION*

We are concentrating to provide adequate security to the sensor networks, which are required both commercially and technically. The sensor nodes of the sensor networks are small, cheap, have limited battery capability and transmission range to perform limited monitoring and sensing functions. Sensor nodes are distributed over a potentially vast geographical area to form a static, multi-hop, self-organizing network. However, also mobile WSNs and mobility within WSN are conceivable. A major benefit of WSN is that they perform in-network processing to reduce large streams of raw data into useful aggregated information.

The Key constraints are providing importance when we design an wireless sensor network is security, lifetime and the transmission delay of the network. Proper design of each of these features depends the system architecture design of a WSN.

Security is typically an important issue in sensor networks includingsensor networks, where the communication medium is broadcast in nature and, hence, an adversary can overhear all messages sent by any user. For this reason, a sender must authenticate the receiver and encrypt any messages it sends. In WSN the channel is assumed to be insecure and the end-points cannot in general be trusted. An attacker may physically pick up sensor nodes and extract sensitive information .Making the sensor nodes "tamper-resistant may be a good solution as it impacts security but it makes the node expensive. Also the limited computing and storage capabilities make modular arithmetic with large numbers difficult and thus asymmetric (public key) cryptography unsuitable.Security is sometimes viewed as a standalone component of a system's architecture, where a separate module provides security.

Toachieve a secure system, security must be attached with every design parameters, since parameters designed without security can become a point of attack. Consequently, security must pervade every aspect of system design. While we designing a scheme for a sensor network, securitysecurity should be incorporated to the mechanisms after design has completed.

An ultimate limitation of building a multi-hop routing topology around a fixed set of base stations is that those nodes within one or two hops of the base stations are particularly attractive for compromise. After a significant number of these nodes have been compromised, all is lost. This indicates that clustering protocols where cluster-heads communicate directly with a base station may ultimately yield the most secure solutions against node compromise and insider attacks.

In this paper we will discuss countermeasures and design considerations for secure routing protocols in sensor networks. For that we first discuss a proposed routing scheme which is modification of the PEGASIS [1],to prolonged the lifetime of the network and then discuss the threats that the scheme may face and trying to resolve a solution to make it secure.

The paper is oriented as follows: In section II we will discuss about literaturepreview,In section III we will concentrate on our proposed scheme and its experimental results and simulation graphs ,In next section we will focus on the attacks against

the scheme ,In section V we are trying to resolve the attacks to make it secure and at last we will draw some conclusion and the future research works that will come as a challenge to the scientists.

## *II. LITERATURE REVIEW*

In this section we will discuss some previous work on the routing protocols and some security management that is already taken for wsn.

Massive experiments and research works were done regarding the lifetime time enhancement routing protocols.Hierarchical or cluster-based routing, originally proposed in wire line networks, are well-known techniques with special advantages related to scalability and efficient communication. As such, the concept of hierarchical routing is also utilized to perform energy-efficient routing in WSNs.Heinzelman*et al.* in [2] developed a cluster-based routing scheme called Low-Energy Adaptive Clustering Hierarchy (LEACH), where in each cluster, member nodes adopt a Time Division Multiple Access (TDMA) protocol to transmit their data packets to the cluster head. After receiving data packets from all its neighboring sensor nodes, a cluster head performs data aggregation and sends the final aggregated packet to the Base Station under the Carrier Sense Multiple Access (CSMA) protocol. LEACH utilizes a more accurate energy model and offers much better performance in terms of energy efficiency and network lifetime. The Power Efficient Gathering in Sensor Information Systems (PEGASIS) scheme proposed in [1] is based on a greedy chain, which starts from the farthest node from the Base Station. By connecting the last node on the chain to its closest unvisited neighbor, PEGASIS greatly reduces the total communication distance and achieves much better energy and lifetime performance than LEACH for different network sizes and topologies.The PEGASIS scheme depends upon a greedy chain formation whereas the LEACH scheme randomizes the leader selection in the network. While the greedy chain cannot always guarantee minimal energy consumption, the randomized leader selection does not take into account the node's capability in being the leader, in terms of its energy content and transmit distance.

Security in sensor networks has been well enumerated in the literature [4].Sensor network security has been studied in recent years ina number of proposals. Kulkarni et al. [5] analyzes on the problem of assigning initial secrets to users in ad-hoc sensor networks to ensure authentication and privacy during their communication and points out possible ways of sharing the secrets.

Secure routing protocols for ad-hoc networks based on symmetric key cryptography have been proposed [7] and for public cryptography is proposed in [4]But the protocols are too expensive in terms of node state and packet overhead and are designed to find and establish routes between *any* pair of nodes.In [6] Karlof et al. thoroughly discussed the problem of secure data transmission for different routing protocols and they conclude that Many sensor network routing protocols have been proposed, but none of them have been designed with security as a goal. They suggested the security goals required forrouting in sensor networks.

## *III.PROPOSED SCHEME*

In this section we modify the PEGASIS algorithm to increase the lifetime of the network here we will first concentrate about the implementation of the scheme followed by the simulation results.

### *A. Problem Formulation and Implementation*

In this paper we have implemented a allocation scheme for the leader selection of the WSN. PEGASIS is power efficient data gathering protocol for wireless sensor network where routing occurs as a greedy chain formation technique. In this work we have compared simultaneously the greedy chain formation with the data gathering using leader allocation strategy. We have assumed that each sensor node in the network bears a initial energy. The sensor nodes are deployed randomly in the network. For a particular node we have allocated initially with certain rounds after selection of that node as a leader. We have simulated the network life time and mean energy of the network using chain formation with leader assigned for fixed rounds. Here we keep track of the leaders i.e. which nodes are selected as leaders and no of rounds they are assigned as leaders. From this statistical analysis we keep track of the min. no. of rounds that a particular node may be posted as leader. Suppose the minimum no. of round is N, in the methodology for leader allocation it set as a restriction for every leader.

We observe that a single node communicates with the base station hence the possibility of collision between the signals may be avoided by leader allocation strategy .Disadvantage of the LEACH protocol [2] where several nodes communicate with the base station either in TDMA or CDMA which we assigned it as leader [8]. So in greedy chain formation we count the possibility of the number of nodes as leader using MATLAB. We have e restricted the no of times a nodes being allowed to be leader. We allocate the least number of counts for a node acting as a leaders shown in

*Table I Count of the Nodes as Cluster head*

| Node ID Number | Count of the Nodes as a Cluster Head. | Mean of the nodes to be a Cluster Head |
|---|---|---|
| 1 | 359 | 145 |
| 2 | 284 | |
| 3 | 119 | |
| 4 | 238 | |
| 5 | 91 | |
| 6 | 97 | |
| 7 | 151 | |
| 8 | 113 | |
| 9 | 104 | |
| 10 | 86 | |
| 11 | 221 | |
| 12 | 126 | |
| 13 | 87 | |
| 14 | 220 | |
| 15 | 95 | |
| 16 | 69 | |
| 17 | 85 | |
| 18 | 248 | |
| 19 | 64 | |
| 20 | 48 | |

For measurement of dissipation of energy different radio model are discussed[3] According to first order radio model the energy dissipated in transmitting ak-bit message over a distance d is given by :

$E_{tx}(K,d) = (e_t + e_d*d^2) * K$ .....(1)

and the amount of energy lost due to reciveing the *k*-bit packet is:

$E_{rx}(K) = e_r * K$……..(2)

where$e_t$is the energy dissipated per bit in the transmitter circuitry and $e_d*d^n$ is the energy dissipated for transmission of a single bit over a distance d, n being the path loss exponent .

*B.Simulation Results*

We have simulated the clustering scheme of data gathering using MATLAB .Considerthe BS is located at (100, 100) in a 100m x 1000m field. We have simulated in C to determine the number of rounds of communication when 10%, 20%, 50% and 100% of the nodes die using direct transmission, LEACH, PEGASIS and Proposed algorithm witheach nodehaving the same initial energy level (0.1mJ). Once a node dies it is considered dead for the rest of the simulation. Our simulations shows that proposed algorithm achieves approximately three times the number of rounds compared to PEGASIS and five times the number of rounds compared to LEACH when 10%, 20%, 50%, and 100% nodes die for a 100m x 100m network.

The Experiment table is shown in the table II as follows

*TableII : Comparative of the Network Lifetime with Node density and initial energy of the Network. FND: First Node Dies, LND: Last Node Dies*

| Node density of the Network | Initial Energy (mJ) | Network Lifetime (No of rounds ) | | | |
|---|---|---|---|---|---|
| | | PEGASIS | | PROPOSED SCHEME | |
| | | FND | LND | FND | LND |
| 100 sensorDeployed in a 50* 50Square field | 100 | 76 | 167 | 78 | 206 |
| | 250 | 200 | 416 | 206 | 465 |
| | 500 | 313 | 780 | 313 | 1029 |
| 200 sensorDeployed in a 50* 50Square field | 100 | 69 | 160 | 69 | 213 |
| | 250 | 153 | 440 | 153 | 380 |
| | 500 | 357 | 771 | 357 | 1028 |

The Network Lifetime enhancement is shown in the comparative figure shown below

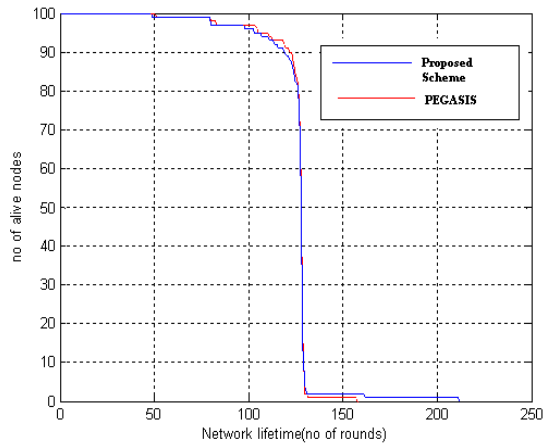


*Fig 1: Comparative plot with 100 no. of nodes over a square area of 50*50 with initial energy 100J*

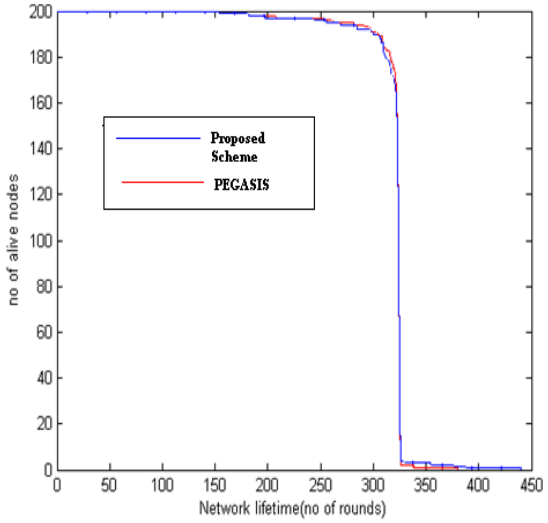


*Fig2: Comparative plot of 200 no. of nodes over a square area of 50*50 with initial energy 250 J.*

Comparative plot of the two schemes are shown with increased number of nodes and initial battery energy which shows significant improvement of network lifetime .as tabulated in table IV and compare in chart in figure 3.

*Table III : Comparison of Network Lifetime in (100m x 100m)square field with BS located at (100m, 100m)*

| PROTOCOL | FND : FIRST NODE DIES | LND : LAST NODE DIES |
|---|---|---|
| DIRECT | 48 | 102 |
| LEACH | 302 | 663 |
| PEGASIS | 388 | 1002 |
| PROPOSED ALGOITHM | 441 | 1115 |

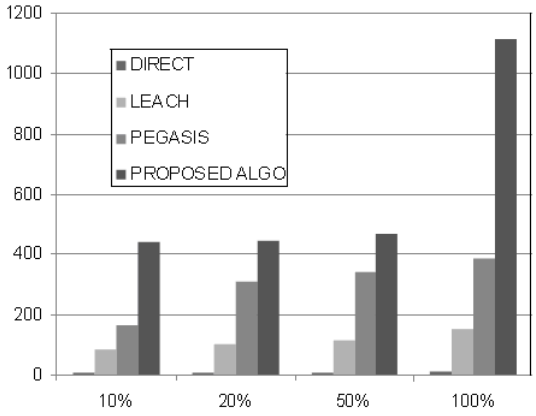


Fig 3:. Percentage of node death and performance results for a 100m x 100m network with initial energy of 0.1J/node

Our performance produces a significant enhancement of Network Lifetime over existing scheme. But it really not save from various attacks so security impact of the scheme is not efficient .

## *IV. ATTACKS ON PROPOSED SENSOR NETWORKSCHEME*

Before focusing on different attacks on the proposed algorithm we will first discuss some assumption underlying about the network scheme we have proposed in the previous section.

*A. configuration of sensor nodes:*

As in wsn all the data are conveying wirelessly so attackers may attack to the radio link between the nodes to inject some hacking data to penetrate the information of the network. And also we also assume that the nodes are not tamper resistance as it tends to add significant per-unit cost, and sensor nodes are intended to be very inexpensive.

*B. Trust Requirements:*

The base station of the network is considered as loyal i.e. it must behave correctly and can be

trusted as it interface a sensor network to the outer world.

*C. Threat Models:*

Several types of attacker are present viz. outsider & insider attackers, mote-class & laptop-class attackers. The outsider attackers are unauthorized person though the insider are authorized person and they may be mounted from either compromised sensor nodes running malicious code or adversaries who have stolen the key material, code, and data from legitimate nodes. The laptop attackers are very massive attackers as they can jam the whole radio links of the sensor network ,have a high bandwidth, low-latency communications channel not available to ordinary sensor nodes, allowing such attackers to coordinate their efforts.

*D. Security Goals:*

Securityprovidesauthenticity, integrity, privacyto a sensor network to covey messages properly in the network and also in the real world. Here we consider eavesdropping which is produced by cloning or rerouting of a data flow as the primary security goal and routing protocols should prevent it.

The effectiveness of a routing protocol in achieving the above goals should degrade no faster than a rate approximately proportional to the ratio of compromised nodes to total nodes in the network.

Now we are elaborate on some shortlisted attacks that our proposed protocol is faced off. The attacks that we will discuss in this section are

- Selective forwarding
- HELLO flood attacks

In this description below we will show how the attacks try to manipulate user data directly and affect our proposed scheme.

*A. Selective forwarding*

When we implement the scheme we always considered that every nodes in the network passed the message to its neighbor faithfully. If a node refuse to forward the message to its neighbor then the balance of the network is pretended. This type of attacks known as Selective forwarding attacks. The worst case occurs when a malicious node drops every massage that it receive. In such case the neighbor nodes may report that it has failed and decide to seek another route. A more precise form of this attack is when an adversary selectively forwards packets. If the attacker implement this attacks in path of data flow then it becomes precise and very effective. Though, it is considerable that adversary ignoring a flow passing through neighboring nodes might be able to emulate selective forwarding by jamming or causing a collision on each forwarded packet of interest but such an effort are tricky at best, and may border on impossible. Thus, we believe an adversary launching a selective forwarding attack will likely follow the path of least resistance and attempt to include herself on the actual path of the data flow. In the next section we will focus on the HELLO flood attacks.

*B.* `HELLO` *flood attack*

HELLO flood attack is introduced in [6]. Here we assume that a node may broadcast HELLO packets to assign themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. This assumption may be false: a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor. Under this circumstances the network is left in a state of confusion. So conveying and propagating the packet between neighboring nodes for topology maintenance or flow control are also subject to this attack. It may be thought of as one-way, broadcast wormholes[9].

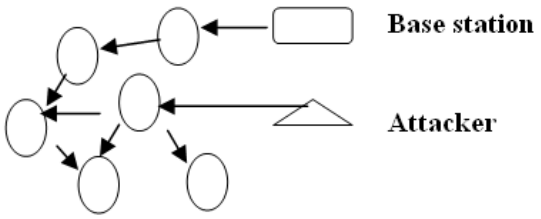


*fig4: an attacker broadcasting hello packets with more transmission power than a base station*

Sensor networks pose some unique challenges regarding the security of the networks as the traditional security management that is implement on traditional networks cannot be applied to the sensor networks because of unlike traditional networks, sensor nodes are often deployed in accessible areas, presenting the added risk of physical attack.existing security mechanisms are inadequate, and new ideas are needed.

## V.*COUNTER MEASURE AGAINST SECURITY THREATS*

In order to meet the application level security requirements, the individual nodesmust be capable of performing,*authentication, privacy,Key establishment and trust setup thus overall a secure routingscheme*. Here we will discuss some counter measure against the security challenges that our proposed scheme faced.

*A. Secure routing:*

Data conveying in proper route is an essential requirement for enabling the communication in the sensor networks. In the previous section we discuss that our scheme faces a major challenges against the Selective forwarding, HELLO flood attacks. Here we will try to resolve this attack to make our protocol secure.

*a. Selective forwarding*

As a solution of the selective forwarding attacks multiple path routing is a good option .Messages routed over multipath whose nodes may have common but link are completely distinguished are completely protected against selective forwarding attacks involving at multiple nodes and still offer some probabilistic protection when over these nodes are compromised.This multipath that may have common nodes but all links are uncommon are known as Braided paths[10].probabilistic protection may be taken against the selective routing attacks using Braided paths. Here nodes are allowed to choose a packet's next hop probabilistically from a set of possible candidates randomly can reduce the control of attackers against the data flow.

*b. HELLO flood attacks*

We assign a particular key to encrypt each request message that a node receivesTo defend against attack. In this way, any node's reachable neighbors can decrypt and verify the REQ message while the attacker will not know the key and will beprevented from launching the attack.But This defense gets less effectiveness when an attacker has a highly sensitive receiver as well as a powerful transmitter.Thus a different way of reliable exchange of messages among nodes and base stations is required so that when any particular node has different route to send data, this problem will be cured.If we assume that, there are a number of base stations in the network who have control over specific number of nodes and also, there are common means of communications among base stations and follows that steps below.

step 1:each nodes uses its new key to exchange messages among them.

step2:Transmission of request massage from base stations to the nearest nodes follows this format :

$$\text{Base station(HCN)} \xrightarrow[\text{REQ}]{\text{Common key}} \text{Nodes}$$

HCN is the base station's one-way hash chain number.Receiving node verifies that the REQ comes from the base station, then it forwards the REQ to its neighbor node in same format using new key.

step3:*Step 3:* When any ordinary node receives this REQ message, it checks the sender ID to verify neighbor, *then it* decrypts and authenticates the sender with computed new key. If the message sender is valid, it replaces the HCN with the new value and encrypts the REQ message with its new keyand broadcasts the newly encrypted message.

The whole process is described it figure 5 considering four base stations with their communication range and sensor nodes with their communication range.

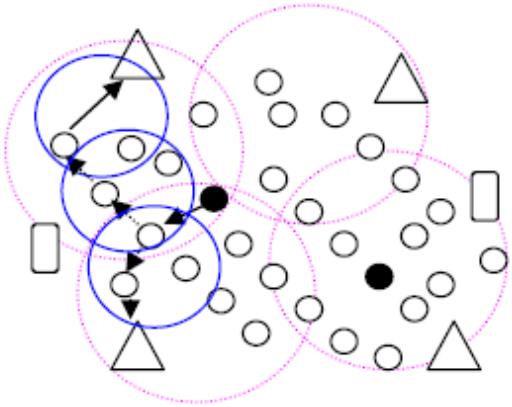

fig 5: Ordinary node gets REQ message from compromised node but does not forward message to it, rather it sends message to its verified neighbor by alternative routes

*B.Authentication and Privacy:*

Here we focus our attention on the problem of assigning initial secrets to users in sensornetwork so that they can use those secrets to ensure authentication and privacy during their communication. As in sensor network all the in formations are exchanging wirelessly so the security of the information may be easily penetrated so a sender must authenticate the receiver. The sender and receiver may be processed to a secure communication by using a common shared key. But it is not an efficient solution.Clearly, if we require that the secret shared between twousers is not known to any other user in thenetwork, then each user must maintain n-1 secrets where nis the number of users. To reduce the number of secrets, the user are allowedto share a collection of secrets, and require thatno other user in the network knows all the secrets in thatcollection. Clearly, in this situation, it would be possible forthe users to use a combination of these secrets to ensure privacy andauthentication.

*C. Key establishment and trust setup:*

Key establishment and trust setup is one of the primary requirement to establish a sensor network setting up. Network shared key is the simplest but the inefficient solution regarding this challenge. Our approach is to preconfigured the network with a shared unique symmetric key between each pair of nodes. Here we consider *n*nodes, each node needs to store *n*- 1 keys, and $n * (n-1)/2$ keys need to be established in the network.

Bootstrapping keys is used for trust setup station is where each node needs to share only a single key with the base station and set up keys with other nodes through the base station. In this protocol the network may incorporate tamper-resistant packaging for the base station, ameliorating the threat of physical attack.

## *VI.CONCLUSIONS*

So from the compact discussion it is clear that it the security that must be considered as the primary constraint for designing a genuine wsn as Security plays a crucial role in the proper functioning ofwireless sensor networks.Though Many other problems also need further research. One is how to secure wireless communication links against eavesdropping, tampering, traffic analysis, and denial of service and also to managing propagation delay of the network but we areoptimistic that much progress will be made on all ofthem.

## REFERENCES

[1] Lindsey, S., Raghavendra, C.S. : PEGASIS: Power Efficient Gathering in Sensor Information Systems, In Proceedings of IEEE ICC 2001 (2001) 1125-1130

[2] Wendi Heinzelman, AnanthaChandrakasan and Hari Balakrishna, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks", In Proceedings of 33rd Hawaii International Conference on System Sciences, Jan. 2000, pp. 1-10

[3] AyanAcharya, AnandSeetharam, Abhishek Bhattacharyya, MrinalKantiNaskar, "Balancing Energy Dissipation in Data Gathering Wireless SensorNetworks Using Ant Colony optimization",10th International Conference Distributed Computing and Networking-ICDCN 2009, pp437-443, Jan 3-6,2009.

[4] L. Zhou and Z. Haas, "Securing ad hoc networks," IEEE Network Magazine, vol. 13, no. 6, November/December 1999.

[5] S. S. Kulkarni, M. G. Gouda, and A. Arora, "Secret instantiation in adhoc networks," Special Issue of Elsevier Journal of Computer Communications on Dependable Wireless Sensor Networks, pp. 1–15, May2005.

[6] C. Karlof and D.Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 1(2–3):293–315, September 2003

[7] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," Department of Computer Science, Rice University, Tech. Rep. TR01-383, December 2001.

[8] AyonChakraborty, Swarup Kumar Mitra, and M.K. Naskar, "AnEfficient Hybrid Data Gathering Scheme in Wireless Sensor Networks", ICDCIT 2010, LNCS 5966, pp. 98–103, 2010.

[9] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless Tech. Rep. TR01-384, June 2002.

[10] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *MobileComputing and Communications Review*, vol. 4, no. 5, October 2001