International Journal of Information Technology and Knowledge Management (ISSN: 0973-4414) July-December 2012, Volume 5, No. 2, pp. 477-483

A 3-tier Heterogeneous Secure Routing protocol for Wireless Sensor Network

Dinesh Singh[1], Parvinder Singh[2], Vikram Singh[3]
[1] [2] DeenbandhuChhotu Ram University of Science & Technology, Murthal (Sonepat), India-131039
[3]Chaudhary Devi Lal University, Sirsa, India
dinesh.madhav@gmail.com,parvinder23@rediffmail.com,vikramsinghkuk@yahoo.com

Abstract: Security is very critical parameter in sensor networks. Securing the WSN needs to make the network support every security property. Security attack is a concern for wireless sensor networks because of usage of very low capacity devices in the systems and physical accessibility to sensor nodes. Therefore to prevent confidential information from being stolen, it is important to provide secure communications between sensor nodes and base stations. This paper presents, a 3-tier heterogeneous secure routing protocol based on LEACH. This protocol is free from all threats which are based on the identity crisis. Threats such as sinkhole, selective forwarding, hello floods etc. can be identified and resolved with this proposed scheme.

Keywords: Wireless Sensor Networks, Sensor Nodes, Heterogeneous approach, Secure Routing, Cluster Head(CH)

I. INTRODUCTION

A wireless sensor network (WSN) is formed by one or more base stations and a large number of sensor nodes to monitor the objects of interest or environmental conditions such as sound, temperature, light intensity, humidity, pressure, motion and so on through wireless communications. Due to distributed nature of these networks and their deployment in remote areas, these networks are vulnerable to numerous security threats that can adversely affect their proper functioning. Since the sensor nodes are deployed in open communication environments, they can easily be attacked during data transmission. The attackers can eavesdrop on its communication channel, inject bits in the channel, replay previously stored packets and much more.

Security requirements and possible attacks in WSNs:
The goal of security services in WSNs is to protect the information and resources from attacks and misbehaviour. Security requirements in WSNs include the following [3]:
Confidentiality means restricting data access to authorized personnel.
Integrity ensures that the receiver receives unaltered data in transit by any unauthorized personnel.
Authentication ensures that the communication from one node to another node is genuine.
Availability ensures that the desired network services are available even in the presence of denial of service attacks.
Data freshness ensures that the recent data is available without any replay of old messages by unauthorized personnel**.**
Self-organization means nodes should be flexible enough to be self-organizing and self-healing (failure tolerant).

Possible attacks in WSNs:
WSNs are vulnerable to various types of attacks as explained below:
Spoofed, altered, or replayed information:
By spoofing, altering or replaying routing information, adversaries can achieve a number of motives like creating routing loops, extending or shortening routing paths, attracting or repelling network traffic, increasing end- to-end latency, partitioning the network, generating false error messages, etc.
Selective forwarding:
An honest node would always faithfully forward the received messages to its destination. However, a malicious node would refuse to forward certain messages and simply drop them, ensuring that the message doesn't reach the intended destination. This is called selective forwarding attack.
Sinkhole attack:
In sinkhole attack, a compromised node is made to look very attractive to the surrounding nodes with respect to the routing algorithm. Hence a metaphorical sinkhole is created with the adversary at the centre.
HELLO flood attack:
Many protocols require broadcasting HELLO packets by the sensor nodes to announce it to the neighbours within their transmission range. But an adversary could flood false HELLO packets.
Sybil Attack:

A single node presents multiple identities to the other nodes in the network. Routes believed to be passing through multiple nodes would actually be passing through the same adversary node and hence thereby running the risk of an endless loop.

Wormholes Attack:

An adversary tunnels messages received in one part of the network over a low latency link and replays them in a different path. Wormhole attack normally involves two distant malicious nodes, misleading others to understate the distance between them by relaying packets along an outer channel, which is available only to the attacker.

II. RELATED WORK

LEACH [5] proposed by Heinzelman et al is a self-organizing, adaptive clustering protocol that uses randomization to distribute the energy load evenly among the sensors in the network. It is vulnerable to a number of security attacks, including jamming, spoofing, replay, etc. However, because it is a cluster based protocol, relying fundamentally on the CHs for data aggregation and routing; attacks involving CHs are the most damaging. If an intruder manages to become a CH, it can stage attacks such as sinkhole and selective forwarding, thus disrupting the workings of the network.

Sec-LEACH [6] provides an efficient solution for securing communications in LEACH. It used random-key pre distribution and μ TESLA for secure hierarchical WSN with dynamic cluster formation. It has fixed key pool and key distribution is static. So that keys can be identified after some certain time by the outsider and he can misuse the keys. FLEACH [7] provides secured node to node communication in LEACH-based network. It used random key pre-distribution scheme with symmetric key cryptography to enhance security in LEACH. FLEACH provides authenticity, integrity, confidentiality and freshness to node-to-node communication. But it is vulnerable to node capturing attack.

This is the first modified secure version of LEACH called S-LEACH [8], which investigated the problem of adding security to cluster-based communication protocol for homogeneous wireless sensor networks consisting of sensor nodes with severely limited resources. J. Ibriq et al. [9] proposed a secure hierarchical energy efficient routing protocol (SHEER) which provides secure communication at the network layer. To secure the routing, it implements HIKES a secure key transmission protocol and symmetric key cryptography. They have compared the performance with the secure LEACH using HIKES. This protocol is based on LEACH protocol; named Authentication confidentiality cluster based secure routing protocol [10]. It uses both public key (in digital signature) and private key cryptography. This protocol deals with interior adversary or compromised node. Because of the high computational requirement (use of public key cryptography), it is not efficient for the WSNs.

III. MOTIVATION

WSNs are prone to failure and malicious attacks because of their physically weakness. A normal node is very easy to be captured to become an adversary node or by inserting a vulnerable node in the network. The malicious nodes try to disrupt the network operation of packet forwarding or will try to consume the resources of the nodes by making them believe that the packets are legitimate. This node will not cooperate in the network operation resulting in the malfunction of the network operation. This happens because any device within the frequency range can get access to the data. So, we need a secure way to protect the network.

IV. PROPOSED SCHEME

We proposed a 3-tier heterogeneous secure routing protocol, which deals with security heterogeneity, based on LEACH. In WSNs, there are a number of sensor nodes (SNs) and a base station (BS).Symmetric key scheme is used for communication. A pair-wise key is assigned to each node pair called Two_way_keys. An associate will use the key common with corresponding CH to communicate with it. CH will use MC (manufacturing code) to communicate with BS.

A. Assumptions

- BS has no constraints regarding memory, computations and energy. It is BOSS for all SNs.
- Network is homogeneous with respect to memory, communicational ability and computational ability of each sensor.

- Heterogeneity in Security: There are two types of nodes-Normal nodes and High Security Nodes. All the high security nodes are trusted and are assumed to be temper proof. They can always be relied upon during the entire network lifetime.

- Every SN is imprinted with a unique code called Manufacturing Code (MC) and a Hash code .MC is used as the private key for the sensor node. It is assumed to be 64 bits in length. Hash code is used to generate the new keys for the SNs.

We talk about the type of threats-Threat0, Threat1, Threat2 and Threat3.

- Threat0 is a malicious node that does not have any valid information and wants to start communication. It can be identified and banned at the time of validation process of hello packets received by BS from each SN.

- Threat1 is a malicious node that has a valid id but code and keys are invalid. It can be identified and banned at the allocation time of CH.

- Threat2 node has a valid id and valid code. So, it can be identified and can be banned. Such nodes send alerts against their associates if they are the CH in present round otherwise it tells the wrong data to their corresponding CH. Once BS receives any alerts from the network, it asks the concerned node to prove its authenticity by sending its key ring which is already stored with the BS. If the sent key ring does not match to that with BS, the node is destined to be banned.

- Threat3 node has a valid id, valid code and valid keys. It can be identified and banned with the matching of renewed keys with the hash code of that particular node with BS. If given information is matched then BS makes fake entry in fake list else ban that malicious node.

B. Procedure:

Setup phase

$S \rightarrow BS: {}^{MC}(id)_{MC}$

If $S_i(id) \in$ list of ids of BS then

BS will generate the random keys R for communication; otherwise ban (S_i).

$BS \rightarrow S: {}^{MC} (id_S, nbr\_list, R)_{MC}$

Cluster formation phase

$CH \rightarrow S: {}^{MC}(id)_{MC}$, adv

$Si \rightarrow CH: {}^{MC}(id_{si}, id_{CH})_{MC}$, join_msg

If $CH(R)==S_i(R)$

Join each other

Steady phase

$S_i \rightarrow CH: {}^{R}(id_{Si}, id_{CH}, d_{Si})_R$

Reliable Data= (d_{HS}) if there is any HS in the cluster; otherwise

Reliable Data= (d_{CH})

P_{error}= Reliable Data- d_{Si}

If $d_{Si} <= P_{error}$ then

$CH \rightarrow BS: {}^{MC} (id_{CH}, id_{Si}, F(...d_{si}...))_{MC}$

If there is a malicious node then alert message is send to BS; it will ask a packet to the alerting nodes i.e. both types of nodes (CH and associates).

$BS \rightarrow CH/S_i: ({}^{MC}(id_{CH}, id_{Si}, MC, hashed(R))_{MC})$, ask_ packet

If information mismatched then ban (CH/Si); otherwise make fake alert entry.

Keys Refreshment

Set key_usage_counter=0

If key_usage_counter >threshold value

R = hash function(R)

Assign R to all sensor nodes and send back to BS.

The various **symbols** denote:

S, CH, HS, BS: All sensor nodes, cluster head, High Security nodes and Base Station respectively

R: Random keys used for two way communication

S_i: A particular sensor node

➔,→ : Broadcast and unicast, transmissions respectively

$^{Encryption\ key}$ (packet) $_{Decryptionkey:}$ This packet is encrypted and decrypted by the same key because symmetric key cryptography is used.

Node x's id

d_x : Sensing report from node x.

adv, join_msg, ask_packet: string identifiers for message types

F: Data aggregation function

P_{error}: Permitted error

V. SIMULATION AND RESULTS

A. Performance Metrics

Following performance matrics are used for the simulation:

a. Network lifetime

The time unless the last node is dead is called the lifetime of network. It is the time span from the deployment to the instant when the network is considered non-functional.

b. Energy consumption per round

Energy consumption is the sum of all computational, communicational energy dissipated in the network in each round. It is calculated as the average energy consumed during the network lifetime.

B. Simulation Scenarios

At the setup time of the network, some malicious nodes are identified:

△ Malicious Node ★ Cluster Heads .....Link between CH and associate

○ Normal Node ○ High Security Nodes ○ A node sending alert messages

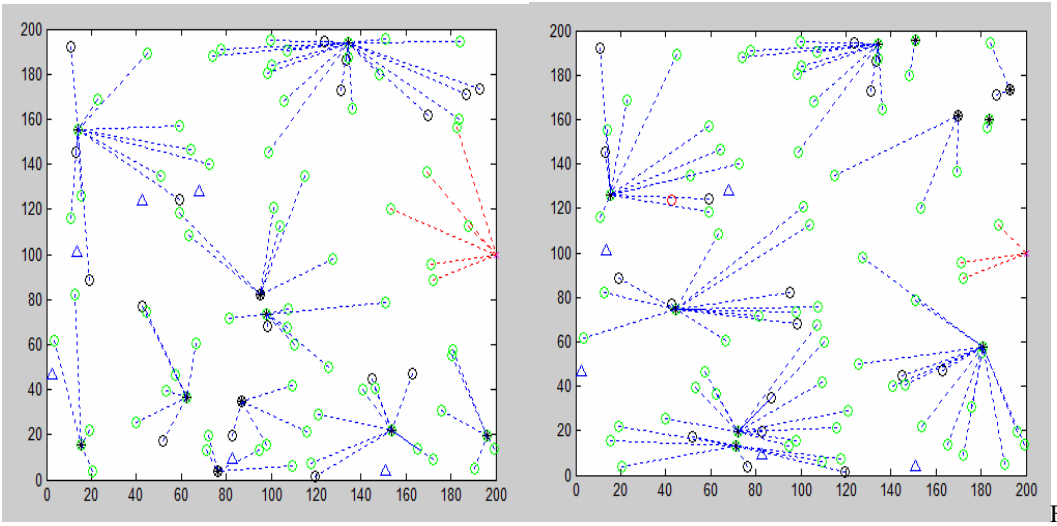

Figure 1: Scenario 1

Figure 2: Scenario 2

In scenario 1, initially all malicious nodes are identified with their invalid id, code and keys. Black circle shows the high security nodes which are more trust-worthy. In scenario 2, a malicious node gets the correct id, code and keys. That node sends alert messages for other nodes. If it is a cluster head, then it communicates wrong data of all associates nodes. After applying the proposed scheme that malicious node is identified as in scenario 1. If a node sends alert messages more than some threshold value then BS asks a packet from the alerting nodes and that node which are alerting them. In ask packet, id, code, and hashed keys are required then BS compares these values as its own. If there is any mismatch for a particular node then ban that node.

C. Results

Parameter	**Value**
Field dimension	200*200
BS location	(200,100)
Numbers of Sensors	100
High Security Nodes	20
Encryption/Decryption	0.168 nJ
$E_{INITIAL}$	0.5 J
E_{ELEC}	50 nJ
E_{AMP}	100 pJ
E_{DA}	5 nJ
Package Length	4000 bits
Sensor Node's id	32bits
Sensor Node's code	64bits
Two _way_ Keys	64bits

Table : Simulation Parameters

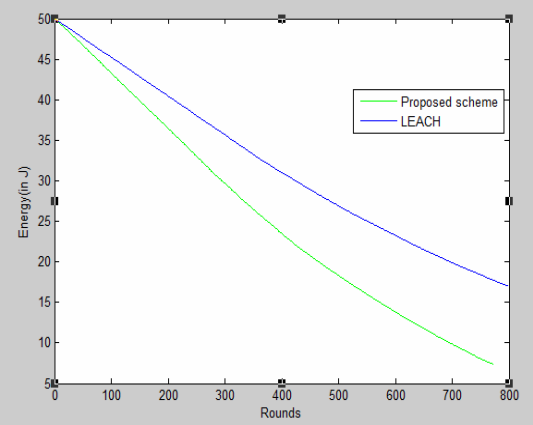

Figure 3: Energy consumption

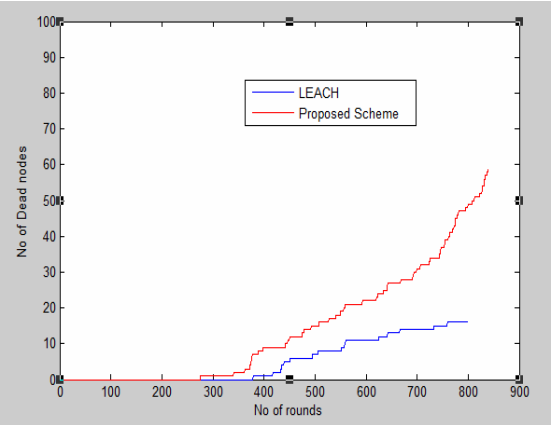

Figure 4: Network lifetime

D. Comparison Tables:

The following is the performance comparison table of the impact of 3-tier Heterogeneous secure scheme with few existing secure routing protocols:

Protocol	**Authenticity**	**Confidentiality**	**Integrity**	**Freshness**
F-LEACH	✓		✓	
SLEACH	✓		✓	
SHEER	✓	✓	✓	✓
Sec-LEACH	✓	✓	✓	✓
3-tier Heterogeneous secure scheme	✓	✓	✓	✓

TABLE 1: PERFORMANCE COMPARISION OF PROPOSED PROTOCOL WITH EXISTING SECURE ROUTING PROTOCOLS BASED ON SECURITY GOALS

Secure Protocol	**Alter/ Replay**	**Selective**	**Sinkhole**	**Sybil**	**Wormhole**	**Hello**	**Outsider**	**Overhead in Key management**
F-LEACH	✓			✓		✓		Medium
SLEACH	✓		✓			✓	✓	High
SHEER	✓	✓		✓		✓	✓	Very High
Sec-LEACH	✓	✓		✓		✓		Medium
3-tier Heterogeneous secure scheme	✓	✓	✓	✓	✓	✓	✓	Medium

TABLE 2: PERFORMANCE COMPARISION OF PROPOSED PROTOCOL WITH EXISTING SECURE ROUTING PROTOCOLS BASED ON PREVENTION OF SECURITY ATTACKS

In Energy consumption figure, there are some trade-offs between security and energy, but it does not shows much difference. This novel scheme provides more security than the LEACH at the less cost of energy. In Network lifetime figure, due to high security more energy will be dissipated and hence the dead nodes are more than LEACH.

6. CONCLUSION AND FUTURE WORK

In this paper, Symmetric key management scheme is used. All computations, like key generation and distribution, are done by BS. Manufacturing code is a more secured key used for encryption and decryption of messages being sent on the link between any node and BS. There's some trust- worthy nodes that avoid node compromised problem. This protocol is free from all threats which are based on the identity crisis. Threats such as sinkhole, selective forwarding, hello floods etc. can be identified and resolved as per the proposed scheme. To provide more security, asymmetric cryptography may be used with the symmetric environment. Hybrid cryptography surely will increase the time of cryptanalyst.

REFERENCES

[1] Ukil A.,"Security and Privacy inWireless Sensor Networks", Smart Wireless Sensor Networks, Intechweb, Croatia, 2010.

[2] Manju V.C.,"Study of security issues in wireless sensor network", International Journal of Engineering Science and Technology (IJEST). ISSN: 0975-5462 Vol. 3 No.,10 October 2011.

[3] Pandey A. et.al,"A Survey on Wireless Sensor NetworksSecurity", International Journal of Computer Applications (0975 – 8887)Volume 3 – No.2, June 2010

[4] Karlof C., Wagner D.," Secure routing in wireless sensor networks: attacksand countermeasures", proceeding in, Ad Hoc Networks 1(2003), 293–315, ELSEVIER.

[5] Heinzelman W., Chandrakasan Anantha P., Balakrishnan H., "Energy-Efficient Communication Protocol for Wireless Micro sensor Networks", Proceedings of the Hawaii International Conference on System Sciences, Maui, Hawaii. January 4-7, 2000.

[6] Oliveira L. B. et.al, "Secleach - a random key distributionsolution for securing clustered sensor networks". InProc. of the Fifth IEEE International Symposium onNetwork Computing and Applications, pages 145–154,Washington, DC, USA, 2006. IEEE Computer Society.

[7] Oliveira L.B. et.al," SecLEACH – A Random Key Distribution Solution for Securing Clustered Sensor Networks", proceeding of the Fifth IEEE International Symposium on Network Computing and Applications (NCA'06) 0-7695-2640-3/06 $20.00 © 2006, IEEE.

[8] Abdullah M.Y., Hua G.W,"Cluster-based Security for Wireless Sensor Networks", proceeding of the International Conference on Communications and Mobile Computing2009, IEEE.

[9] Ibriq J. and Mahgoub I.," A secure hierarchical routing protocol for wireless sensor networks", In Proc. 10th IEEE International Conference on Communication Systems, pages 1–U˝ 6, Singapore, October 2006.

[10] Srinath R., Reddy A. V., and Srinivasan R.,"Ac: Cluster based secure routing protocol for wsn", In Proc. of the Third International Conference on Networking and Services, page 45, Washington, DC, USA, 2007. IEEE Computer Society.