ISSN:0975-9646



# A Novel Approach for Secured Communication in WSN Using Dynamic Low-Weight Keys

Urmila Devi

*Computer Science and Engineering Department*
*DCRUST, Murthal, Sonepat,*
*Haryana, India*

***Abstract*** **— This paper presents, a 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 as per the proposed scheme. We also discussed some of the available secure routing protocols and most common attack patterns against wireless sensor networks.**

***Keywords***— **Wireless Sensor Networks, Secure scheme based on LEACH, Heterogeneous approach, Keys.**

## 1. 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. Securing the WSN needs to make the network support all security properties: confidentiality, integrity, authenticity and availability [1]. Security attack is a concern for wireless sensor networks because:

- Usage of minimal capacity devices in parts of the systems
- Physical accessibility to sensor and actuator devices
- Wireless communication of the system devices

So to prevent confidential information from being stolen, it is important to provide secure communications between sensor nodes and base stations.

### *A. Security requirements and possible attacks*

The goal of security services in WSNs is to protect the information and resources from attacks and misbehaviour. Security requirements in WSNs are as follows [2]:

TABLE 1 SECURITY REQUIREMENTS

| **Security Requirements** | **Description** |
|---|---|
| Confidentiality | The content of the message can only be received by a authorised sender and the intended receiver. |
| Authentication | It ensures that the communication from one node to another node is genuine, i.e., a malicious node cannot masquerade as a trusted network node. |
| Availability | It ensures that the desired network services are available even in the presence of denial of service attacks. |
| Integrity | It ensures that the receiver receives unaltered data in transit by any unauthorized personnel. |
| Data freshness | Data freshness ensures that the recent data is available without any replay of old messages by unauthorized personnel**.** |

TABLE 2 ROUTING ATTACKS IN WSN

| **Attacks** | **Description** |
|---|---|
| Spoofed, altered, or replayed routing information | Create routing loop, attract or repel network traffic, extend or shorten source routes, generate false error messages, etc. |
| Selective forwarding | In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. A simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet [4]. |
| Sinkhole attacks | Attracting traffic to a specific node, e.g. to prepare selective forwarding. |
| Sybil attacks | A single node presents multiple identities, allows to reduce the effectiveness of fault tolerant schemes such as distributed storage and multi-paths, etc. |
| Wormhole attacks | Tunnelling of messages over alternative low-latency links to confuse the routing protocol, creating sinkholes, etc. |
| HELLO floods | An attacker sends or replays a routing protocol's HELLO packets with more energy. |

TABLE 3 POSSIBLE ATTACKS ON WSN LAYERS [3]

| WSN Layer | Types of Attacks |
|---|---|
| Physical Layer | Denial of service attack |
| Data Link Layer | Denial of service attack |
| Network layer | Denial of service attack, Wormholes, Sinkholes, Sybil attacks. |
| Transport Layer | Denial of service |
| Application Layer | Malicious Node |

## 2. RELATED WORK

LEACH [5] is proposed by Heinzelman et al. It 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 μTESLA 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 SLEACH [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.

## 3. 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.

## 4. PROPOSED SCHEME

We proposed a hierarchical protocol, which deals with security heterogeneity, based on LEACH. In the network, there are a number of sensor nodes (SNs) and a base station (BS).Symmetric key scheme is used. There is 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 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**

1. S➔BS: $^{MC}(id)_{MC}$
2. If $S_i(id) \epsilon$ list of ids of BS then

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

3. BS➔S: $^{MC}$ ($id_S$, nbr_list, R) $_{MC}$

**Cluster formation phase**

4. CH➔ S: $^{MC}(id)_{MC}$, adv
5. Si➔ CH: $^{MC}(id_{si}, id_{CH})_{MC}$, join_msg
6. If CH(R)==$S_i$(R)
   Join each other

**Steady phase**

7. $S_i$➔CH: $^{R}(id_{Si}, id_{CH}, d_{Si})_R$
8. Reliable Data= ($d_{HS}$) if there is any HS in the cluster; otherwise
   Reliable Data= ($d_{CH}$)
9. $P_{error}$= Reliable Data- $d_{Si}$
10. If $d_{Si} <= P_{error}$ then
11. CH➔BS: $^{MC}$ ($id_{CH}$, $id_{Si}$, F (...$d_{si}$...))$_{MC}$
12. 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).
13. BS➔CH/$S_i$: ($^{MC}(id_{CH}, id_{Si}, MC, hashed(R))_{MC}$), ask_ packet
14. If information mismatched then ban (CH/Si); otherwise make fake alert entry.

**Keys Refreshment**

15. Set key_usage_counter=0
16. If key_usage_counter >threshold value
    R = hash function(R)
17. 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) $_{Decryption\ key:}$** This packet is encrypted and decrypted by the same key because symmetric key cryptography is used.

**$id_x$:** 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

*1. Setup Phase:*

Each sensor node sends a Hello_Packet to BS containing its id encrypted with its own MC and can be decrypted with only that MC (Manufacturing Code) at the BS. BS obtains locations and neighbour lists for all nodes using Hello_Packet. For all neighbours a random key will be generated that is used for the two way communication. BS sends packets that contain the encrypted id, neighbour keys for each sensor node. Each node will decrypt this packet using manufacturing code to obtain the paired keys and neighbour list.

*2. Cluster Formation Phase* :

Similar to LEACH, CH will be formed and each node will select the nearest CH, with whom it shares at least one key, as its own BOSS. In case no keys are shared with the nearest CH, an alert is generated by either of the communicating nodes and the associate starts looking for another CH with whom keys might have been shared.

*3. Communication Phase:*

After cluster formation, node will use the key common with the corresponding CH to communicate with it. CH will aggregate the data and sends to BS. Before sending to BS, CH will check the integrity of the data. If there is a HS in the cluster then its data will be regarded as reliable data otherwise the data from the CH itself will be called reliable. A predetermined amount of deviation from the reliable data will be permissible for all other nodes in the cluster. The nodes which send data out of the range of the permitted deviation will be considered a potential threat. This will be only a partially checking. An alert will be generated as a reaction to such an event. The id of such a node will be sent to BS along with the id of CH itself. Then, BS fully confirms whether such node is compromised or not. BS will send an ASK_PACKET to the pointed node. This node will have to send back its id, code (manufacturing code), keys and hash code to obtain an authenticity certificate from BS.

*4. Key Refreshment:*

In the proposed scheme, the keys are dynamically updated after a maximal usage. The keys are renewed only after usage not on the basis of time-bound with the help of hash function.

*C. Flow Chart:*

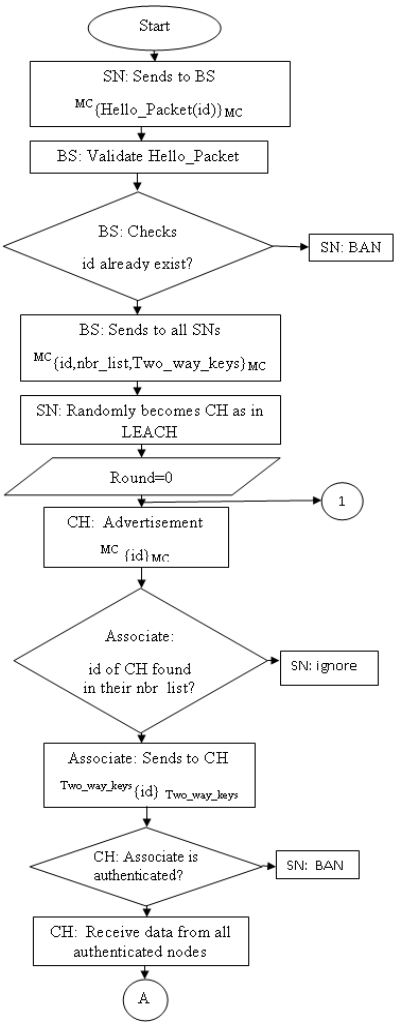


Figure 1: Flow-chart1

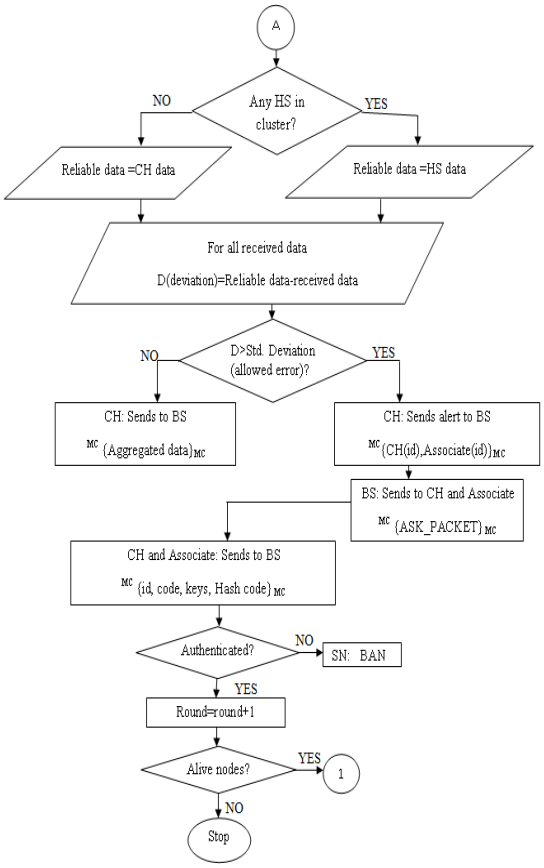


Figure 2: Flow-chart2

## 5. Simulation And Results

### A. Performance Metrics

*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. Comparison Tables

TABLE 4
SECURE ROUTING PROTOCOLS ANALYSIS BASED ON SECURITY GOALS

| Protocol | Authenticity | Confidentiality | Integrity | Freshness | Availability |
|---|---|---|---|---|---|
| F-LEACH | ✓ | | ✓ | | |
| SLEACH | ✓ | | ✓ | | |
| SHEER | ✓ | ✓ | ✓ | ✓ | |
| Sec-LEACH | ✓ | ✓ | ✓ | ✓ | |
| Proposed Scheme | ✓ | ✓ | ✓ | ✓ | |

TABLE 5
SECURE ROUTING PROTOCOLS COMPARISON BASED ON PREVENTION OF SECURITY ATTACKS

| 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 |
| Proposed Scheme | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Medium |

### C. *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

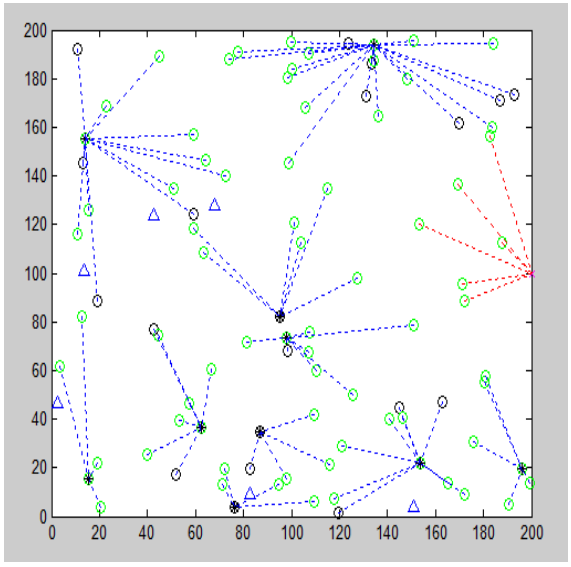

Figure 3: Scenario 1

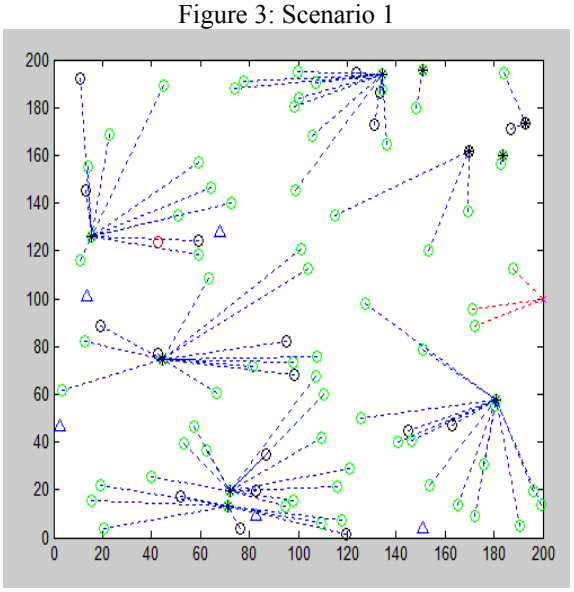

Figure 4: Scenario 2

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 told 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.

### D. *Results*

Table 6 Simulation Parameters

| 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 |

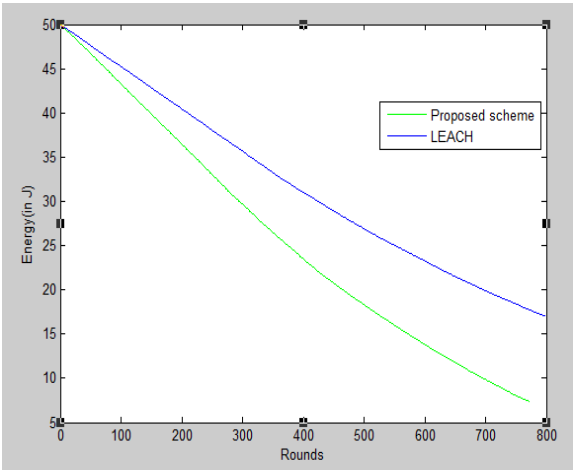


Figure 5: Energy consumption

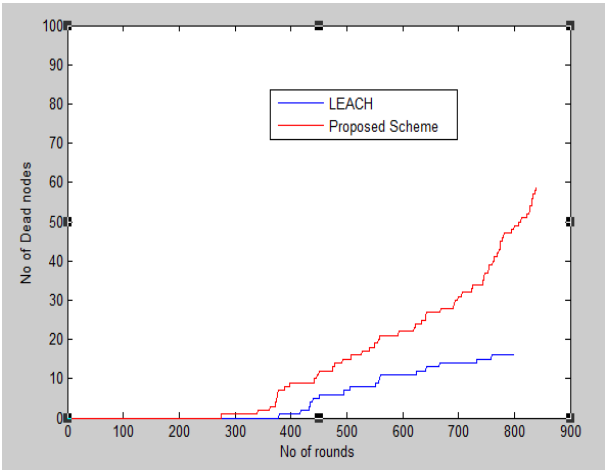


Figure 6: Network lifetime

In figure5, there are some trade-offs between security and energy. But it shows not much difference. This novel scheme provides more security than the LEACH at the less cost of energy. In figure 6, due to high security more energy will be dissipated. That's why our 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 is 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. In future reference, to provide more security, asymmetric cryptography may be used with the symmetric environment. Whenever a CH wants to talk with the BS, it may use public keys that may be broadcasted by BS at the setup time. Hybrid cryptography surely will increase the time of cryptanalyst.

## 7. REFERENCES


[1] Ukil A.," Security and Privacy in Wireless 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 Networks Security", International Journal of Computer Applications (0975 – 8887) Volume 3 – No.2, June 2010

[4] Karlof C., Wagner D.," Secure routing in wireless sensor networks: attacks and 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 distribution solution for securing clustered sensor networks". In Proc. of the Fifth IEEE International Symposium on Network 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.


## AUTHOR

**Urmila Devi** had completed her M.Tech in Computer Science and Technology from DCRUST, Murthal, Sonepat, Haryana, India in May, 2012. Her Research interest includes Security in Wireless Sensor Network. She received her B.Tech in Computer Science and technology with Gold Medal from GJUS&T, Hisar, Haryana. She also qualified NET exam. Her research areas are Wireless Sensor Network and MANETs.