A Novel Energy Efficient Mechanism for Secured Routing of Wireless Sensor Network

Anupriya Sharma[1], Paramjeet Rawat[2], Suraj Malik[3], Sudhanshu Gupta[4]

[1] **Computer Science, GBTU, IIMT Engg. College Meerut**
[2] **Computer Science, GBTU, IIMT Engg. College Meerut**
[3] **Computer Science, GBTU, IIMT Engg. College Meerut**
[4] **Computer Science, GBTU, BIT Engg. College Meerut**

Abstract

Large-scale wireless sensor networks are highly vulnerable to attacks because they consist of numerous resource-constrained devices and communicate via wireless links. As wireless sensor networks are continue to grow, so they need an effective security mechanisms. As sensor networks may interact with sensitive data and/or operate in hostile unattended environments, it is imperative that these security concerns must be addressed from the beginning of the system design. However due to inherent resource and computing constraints, security in sensor networks poses different challenges than traditional network computer security. Here we describe an energy efficient security scheme for sensor networks that is designed for long lived networks. Primary features of our scheme include autonomously computing administration keys and dynamically mapping of sensor nodes to set of keys. The scheme scales well in the size of the network and supports dynamic setup and management of arbitrary structures for secure communications in large-scale wireless sensor network. A salient feature of the security scheme is that, it supports source authentication as well as end-to-end authentication, integrity of communication, efficiently addition of the sensor nodes to the network dynamically.

Keywords: *wireless, sensor, security, vulnerability, source authentication, energy efficient, integrity*

1. INTRODUCTION

A wireless sensor network is a network of simple sensing devices; which are capable of sensing some changes of incidents/parameters and communication with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. Since sensor nodes are tightly constrained in processing ability, storage capacity and energy and secured routing over Wireless Sensor Networks (WSN) presents a unique challenge. Mature solutions [1] for key management are too complex for wireless sensor networks, as the resources required would quickly exhaust the small sensors. The suitability of these WSNs for military applications and the deployment of these networks in hostile environments have brought the challenge of securing the communication between these extremely resource constrained devices. In addition to battlefield deployment, there are a number of future applications that will require a high level of security.

The extensive growth in using sensor networks in a wide variety of applications ranging from health care to warfare is fueling extensive research in securing these networks. The characteristics of sensor nodes and sensor networks including lack of physical protection and the resource constrained nature of sensors render most existing security solutions developed for other networks (e.g. Public-Key-based solutions) infeasible for sensor networks.

The tradeoff between managing acceptable levels of security and conserving network energy for sensor network operation is a challenging task. Recently, a number of security schemes have been developed for sensor networks [2,3,4]. We broadly classify these security schemes for sensor networks into static and dynamic keying based on whether the administrative keys (those used to establish communication keys) are distributed or updated or on the basis of initial network deployment and setup. Unlike static keying, dynamic keying schemes change all keys revealed to an attacker upon node capture.

The major advantage of dynamic keying is enhanced network survivability, so that captured keys are replaced in a timely manner. Our main contribution is purposing an power-efficient and scalable dynamic key management scheme for secured communication over sensor networks. Our scheme is a dynamic key management scheme in which a set of keys is assigned to every sensor node after its deployment and periodic refreshment of network for verifying the nodes which are alive over the lifespan of a network.

2. 2. RELATED WORK

Key management schemes [2,4] in sensor networks can be classified broadly into dynamic or static solutions based on whether re keying (update) of administrative keys is enabled post network deployment. Schemes can also be classified into homogeneous or heterogeneous schemes with regard to the role of network nodes in the key management process. All nodes in a homogeneous scheme perform the same functionality; on the other hand, nodes in a heterogeneous scheme are assigned different roles. Homogeneous schemes generally assume a flat network model, while heterogeneous schemes are intended for both flat and clustered networks. Other classification criteria include whether nodes are anonymous or have pre deployment identifiers and if so, when (pre- post-deployment or both) and what deployment knowledge (location, degree of hostility, etc.) is imparted to the nodes.

2.1 Static Key Management Scheme

These schemes assume that once administrative keys are[2] pre deployed in the nodes, they can not be changed. Administrative keys are generated prior to deployment, assigned to nodes either randomly or based on some deployment information and then distributed to nodes. For communication key management, most static schemes use the overlapping of administrative keys to determine the eligibility of neighboring nodes to generate a direct pair-wise communication key. In order to establish and distribute a communication key between two non-neighboring nodes and/or a group of nodes, that key is propagated one link at a time using previously established direct communication keys. All of the static schemes are homogenous and not reliant on post deployment information. Several techniques have been proposed to make use of deployment knowledge in order to improve static key management. Deployment knowledge may include node locations, neighbor locations, node cluster (or group), as well as the attack probability in certain portions of the network.

2.2 Dynamic Key Management Scheme

Dynamic key management schemes may change administrative keys periodically on demand or on detection of node capture. The major advantage of dynamic keying is enhanced network survivability, since any captured keys are replaced in a timely manner in a process known as re-keying. Another advantage of dynamic keying is providing better support for network expansion, upon adding new nodes, unlike static keying, which uses a fixed pool of keys, the probability of network capture does not necessarily increase. Both homogeneous and heterogeneous dynamic key management schemes have been proposed in the literature. The major challenge in dynamic keying is to design a secure yet efficient re keying mechanism. A proposed solution to this problem is *Jolly et al.'s* approach; key generation and assignment are the responsibility of the base station, while key distribution is performed by the cluster gateways. The proposed scheme requires very few keys to be stored at each sensor node and shared with the base station as well as the cluster gateways.

Re keying involves reestablishment of clusters and redistribution of keys. Although the storage requirement is very affordable, the re keying procedure is inefficient due to the large number of messages exchanged for key renewals**.**

Another researchers Du et al. [5] proposed a novel random key predistribution scheme that exploits deployment knowledge and avoids unnecessary key assignments. It shows that the performance (including connectivity, memory usage, and network resilience against node capture) of sensor networks can be substantially improved. This scheme is based on known deployment points by choosing keys shared with nodes likely to be in close proximity.

Carman et al. [] conducted a comprehensive analysis of various group key schemes. The authors conclude that the group size is the primarily factor that should be considered when choosing a scheme for generating and distributing group keys in a WSN**.**

LEAP

The existing protocol LEAP [6] (Localized Encryption and Authentication Protocol) that provides the security for wireless sensor networks has the following properties:

- The design of the protocol is motivated by the observation that different types of messages exchanged between sensor nodes have different security requirements, and a single keying mechanism is not suitable for meeting these requirements. Consequently, LEAP includes support for establishing four types of keys per sensor node – individual keys are shared with the base station, pair wise keys shared with individual neighboring nodes, cluster keys shared with a set of neighbors, and a group key shared with all the nodes in the network. These keys can be used to increase the security of many non-secure protocols.
- LEAP includes an efficient protocol for inter-node traffic authentication based on the use of one-way key chains.
- A distinguishing feature of LEAP is that its key sharing approach supports in-network processing, while at the same time it restricts the security impact of a node compromise to the immediate network neighborhood of the compromised node.
- The key establishment and key updating procedures used by LEAP are efficient and the storage requirements per node are small.
- LEAP can prevent or increase the difficulty of launching many security attacks on sensor networks.

3. ISSUES WHICH NEED TO BE ADDRESSED

The following characteristics of sensor networks[1] complicate the design of secure protocols for sensor networks and make the bootstrapping problem highly challenging. We discuss the origins and implications of each factor in turn.

3.1 Impracticality of public key cryptosystems

The limited computation and power resources of sensor nodes often makes it undesirable to use public-key algorithms, such as Diffie-Hellman key agreement or RSA signatures. Currently, a sensor node may require on the order of tens of seconds up to minutes to perform these operations. This exposes a vulnerability to denial of service (DoS) attacks.

3.2 Vulnerability of nodes to physical capture

Sensor nodes may be deployed in public or hostile locations (such as public buildings or forward battle areas) in many applications. Furthermore, the large number of nodes that are deployed implies that each sensor node must be low-cost, which makes it difficult for manufacturers to make them tamper-resistant.

3.3 Lack of a-priori knowledge of post-deployment configuration

If a sensor network is deployed via random scattering[7] (e.g. from an airplane), the sensor network protocols cannot know beforehand which nodes will be within communication range of each other after deployment. Even if the nodes are deployed by hand, the large number of nodes involved makes it costly to pre-determine the location of every individual node. Hence a security protocol should not assume prior knowledge of which nodes will be neighbors in a network.

3.4 Limited memory resources

The amount of key-storage memory in a given node is highly constrained. It does not possess the resources to establish unique keys with every one of the other nodes in the network.

3.5 Over-reliance on base stations exposes vulnerabilities

In a sensor network, base stations are few and are much powerful. Hence it may be tempting to rely on them as a source of trust. However this invites attack on the base station and limits the application of the security protocol.

4. PROPOSED WORK

We describe below our assumptions regarding the sensor network scenarios in which our security protocols will be used-

Network and security assumptions:

i. We assume that the sensor network is static, i.e. sensor nodes are not mobile.
ii. The base station, acting as a controller (or key server), is assumed to be a laptop class device and supplied with long-lasting power. The sensor nodes are similar in their computational and communication capabilities and power resources to current generation sensor nodes. The base station is part of a trusted computing environment.
iii. We make the assumption that the communication channel is symmetric.
iv. The sensor nodes can be deployed via aerial scattering or by physical installation.
v. We assume that if a node is compromised, all the information it holds will also be compromised. However we assume the base station will not be compromised.
vi. The sensors nodes are randomly distributed and are not aware of the topology prior to the deployment.
vii. We are not making any trust assumptions on sensor nodes or any assumptions on the capabilities of the adversary.
viii. Sensor nodes remain stationary during the operation of the network.
ix. In addition we assume that the base station is capable of reaching all sensor nodes within its network through broadcast.

The main goal of our protocol is to design efficient security mechanisms for supporting various communication models in sensor networks. The security requirements not only include authentication and confidentiality but also robustness and survivability.
The protocol should also support sensor network optimization mechanisms such as in-network processing. Since the resources of a sensor node are very constrained, the key establishment protocols should be lightweight and minimize communication and energy consumption. It should be possible to add new sensor nodes incrementally to the sensor network.

Our goal is to efficiently source communication among sensor nodes, end-to-end authentication, and confidentiality and integrity attacks in long-lived large-scale sensor networks operating in hostile environment. Our protocol manages two types of keys, one which is shared between individual sensor node and base station and the second which a sensor node is sharing with its neighboring sensor nodes. Node capture attacks, including the capture of sensor nodes are handled through same levels of re-keying (or changing administrative keys). As previously discussed, our protocol provides multiple keying mechanisms that can be used for providing confidentiality and authentication in sensor networks. Sensor nodes are preloaded with a unique sequence number prior to deployment and certain code (initial key) that they will share with base station. Initial communication among nodes and base station is encrypted with these keys that they will share with base station.

We first motivate and present an overview of the different keying mechanisms before describing the protocol used by our protocol for establishing these keys.

As the study reveals that no single keying mechanism is appropriate for all the secure communication that is needed in sensor networks. As such our protocol supports the establishment of two types of keys for each sensor node, an individual sensor node key shared with the base station, a pair wise key shared with another neighboring sensor node. We now discuss each of these keys in turn and describe our reasons for including it in our protocol.

A. Individual key

Every node has a unique key that it shares pair wise[2] with the base station. This key is used for secure communication between a node and the base station

B. Pair wise shared key

Every node shares a pair wise key[2] with each of its immediate neighbors. In our protocol, pair wise keys are used for securing communications that require privacy or source authentication and which provide an end to end authentication.

Key Establishment

We describe the schemes provided by our protocol for sensor nodes to establishment of individual keys and pair wise shared keys for each sensor node. There is a list of notations which are used in our protocol-

1. N is the number of sensor nodes in the network
2. A → B message is transmitting from sensor node A to B.
3. *Key_k* is a key at node k used for communication by the node k.
4. *Encrpt_key* is the encryption key which is shared between any sensor node and base station.
5. *NT_k* is the neighbor table maintained locally by sensor node k in the network.
6. *NT_BS* is the neighbor table maintained at the base station.
7. *KeyTable_BS* is the key table maintained at the base station, which maps the set of keys which are assigned to any sensor node in the network.
8. *AliveTable* is the table maintained at base station to keep the list of alive sensor nodes in the network

4.1 Establishing Individual Node Keys

Every sensor node has a 128 bit secret key that is only shared with the base station. This key is generated and preloaded into each node prior to its deployment. When base station needs to communicate with an individual node *k*, it used that key which is shared with the sensor node. Due to the computational efficiency of base station, the computational overhead is negligible.

4.2 Establishing Pairwise shared keys

A pair wise shared key belonging to a sensor node refers to a key shared only between the node and one of its direct neighbors (i.e. one-hop neighbors). Here we are interested in establishing pair wise keys for sensor nodes unaware of their neighbors until their deployment (e.g. via aerial scattering). Our approach exploits the special property of sensor networks consisting of stationary nodes that the set of neighbors of a node is relatively static and that a sensor node that is being added to the network will discover most of its neighbors at the time of its initial deployment.

Pre-deployment initialization

The pre-deployment phase securely implants the initial key in all nodes. One major advantage of our protocol is that all sensor nodes are preloaded with a unique sequence number. In addition to the unique sequence number, each node is also preloaded with a 128 bit secret key which it shared with the base station. A pre-deployment initialization includes loading the entire set of sensor nodes with the sensor node id's. It is not required that the base station knows the location of the all sensor nodes before or after deployment.

Post-deployment initialization

After deployment the network starts a top-down bootstrapping process beginning at the base station and proceeding downwards to the sensor nodes. The communication message format is following type:

<S_Addr,(key_k(D_Addr),TYPE),Encrpt_key[data]>

Where:

1. S_Addr will contain address of sending node.
2. D_Addr contains the address of the destination.
3. TYPE is the type of message that is being transmitted.
4. Encrypt_key[data] is the encrypted data sent from one node to the other

The different types of communication message used in the key distribution algorithm are:

1. HELLO_BS- is the broadcast message from the base station to all sensor nodes in the network.
2. HELLO_SN - is the broadcast message from any sensor node to all sensor nodes in the network.
3. HELLO_SNREPLY - is the reply of the broadcast message from any sensor node to other sensor nodes in the network.
4. NLIST - this message is generated by any sensor node in the network and it contains the neighbor list of any sensor node in the network.
5. KEYS - this message is generated by the base station and contains the set of keys assigned to any sensor node in the network.

After deployment base station sends a broadcast to all sensor nodes in the network to send their neighbors information. All sensor nodes in the network then broadcast a neighbor discovering hello message in the network. All the sensor nodes which hear message will reply to their immediate neighbor nodes by sending their unique ID to it. Then each sensor node use the secret key to register with the base station by sending their ID and neighbor table information encrypted with shared key with the base station. Upon receiving such messages, the base station registers all sensor nodes and determines the number of valid sensor nodes and accordingly computes suitable set of key values for each sensor node.

ALGORITHM: Key Distribution Algorithm

N : all sensor nodes in the network

1. Set NT_k = Φ
   [where k belongs to N. Neighbor table at the each sensor node is initially empty and size of NT_k is at most |N|.]
2. Set NT_BS = Φ
   [Neighbor table at the base station is initially empty and the size of NT_BS is at most |N|*|N|.]
3. Base station(BS) broadcast message:
   <BS, HELLO, NULL >
   to all nodes to collect the neighbor information in the network .
4. Each node of sensor network broadcast a Hello message: <S_Addr[k], HELLO_SN, NULL> to collect the neighbor information.
5. If a sensor node replies with the message: <S_Addr[j],HELLO_SNREPLY, Node_ID>to other sensor node then it is added to the neighbour list of the previous sensor node.
6. NT_k = NT_k + j
   [where j is the node that is replying to the node k. So its ID is added in the Neighbor table of k.]
7. Then the sensor nodes which requires keys, sends its neighbour information to the base station
   < S_Addr[k] , BS , Encrpt_key [NT_k] >
8. Then Base station updates its neighbour table by adding the ID of node k in its Neighbor Table.
   NT_BS = NT_BS + k
9. Base station sends the set of keys to the sensor nodes.
   <BS, S_Addr[k],Encrpt_key[NT_k]>
10. Base stations updates its Key Table:
    KeyTable = KeyTable + k
    and updates the Alive table:
    AliveTable = AliveTable + k

Then base station sends the set of keys to each sensor node encrypted with the shared key. The base station maintains a key table with it, where it will keep track of the set of keys allocated to each sensor node in the network. Base station also maintains an *AliveTable* by which it will keep track of all alive sensor nodes in the network.

5. PERFORMANCE EVALUATION

In the case of our sensor network the security requirements are comprised of authentication, integrity, privacy (or confidentiality). The recipient of a message needs to be unequivocally assured that the message came from its stated source. Similarly the recipient needs to be assured that the message was not altered in transit and that it is not an earlier message being re-played in order to veil the current environment. Finally all communications need to be kept private so that eavesdroppers cannot intercept, study and analyze and devise counter measures in order to circumvent the purposes of the sensor network. The simulation implements application using the Network Simulator-2 (NS-2) tool and the MannaSim, which is a framework made of a set of base classes that extends NS-2 to simulate sensor networks. The Mannasim Framework is a module for wireless sensor network simulation based on the Network Simulator (NS-2). Mannasim extends NS-2 introducing new modules for design, development and analysis of different wireless sensor network applications. We have taken the observations between 500 to 5000 nodes by incrementing 500 node at each step.

In simulated environment when we scattered 500 node and further randomly add 10 nodes and delete 10 node from the network we measured some standard results of energy radiation

After gathering the data from different observations, following graphs are obtained that compares our receiving energy with receiving energy used in LEAP [7]. This graph shows that energy consumed in our protocol is less than the previous results.

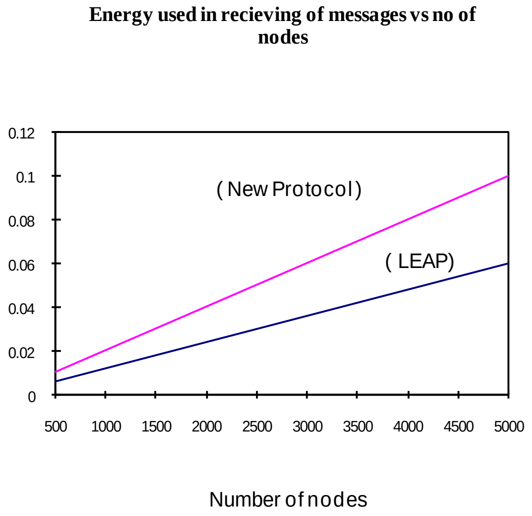

FIGURE 1

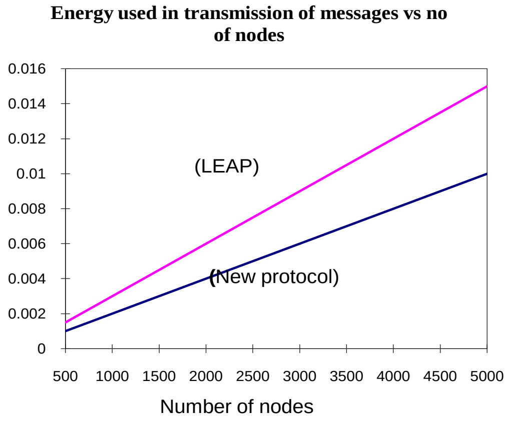

FIGURE 2

RESULT ANALYSIS

Analysis of the communication cost and storage requirement of this new key establishment scheme is described below:

5.1 COMMUNICATION COST

The analysis of communication cost for distributing keys to the sensor nodes depends on the energy used in number of message transmitted and number of message received in the key establishment phase. For establishing the sensor node administrative keys, the average number of message transmited is 1+d where d is density of the network and the average number of message received are equal to 1+d+X, where X is the number of nodes in the transmission range of sensor node in a network of size N. The average communication cost increases with the connection degree of a sensor network.

5.2 STORAGE REQUIREMENTS

In this scheme, a sensor node needs to keep two types of keys. If a node has d neighbors, it needs to store one individual key, d pair wise keys. In a sensor network the packet transmission rate is usually very small. Thus a node could store a reasonable length of key chain. Let d be the number of keys a node stores for its neighbor information. Thus the total number of keys a node stores is d+1. Therefore the total amount of memory needed is 128(1+d)+ e bits, where e is a constant term used to signify the memory used by various things like encryption algorithm, neighbor table etc. Although memory space is a very scarce resource for the current generation of sensor nodes, for a reasonable degree d, storage is not an issue in this scheme. For example, when d = 20, a node stores 21 keys (totally 336 bytes when the key size is 128 bits). Overall, we conclude that the new scheme is scalable and efficient in computation, communication and storage.

5.3 SECURITY ANALYSIS

In analyzing the security of the keying mechanisms, firstly discuss the survivability of the network when undetected compromises occur and then study the robustness of the scheme in defending against various attacks on routing protocols. When a sensor node u is compromised, the adversary can launch attacks by utilizing node u's keying materials. If the compromise event is detected somehow, our scheme can revoke node u from the group efficiently. Basically the base station and every neighbor of node u delete its pair wise key shared with u and update their key set. After the revocation the adversary cannot launch further attacks**.**

Our Pair wise keys provide source authentication as well as end-to-end authentication. The basic scheme for authentication is, every node authenticates a packet it transmits using its own key, which it is sharing with its neighboring nodes. A receiving node first verifies the packet using the same key that it shared with the sending node in the pair wise key establishment phase then authenticates the packet to its own neighbors with its own that it shared with its neighbor's key. Thus a message gets authenticated repeatedly in a hop-by-hop fashion if it traverses multiple hops. The approach provides immediate authentication (node to node) as well as end-to-end authentication.

6. CONCLUSION

Design requirements for security scheme include energy awareness, survivability and localization of attack impact given a highly vulnerable network that mainly operates unattended and scalability to a large dynamic network. One major challenge to dynamic keying schemes is the need for the participation (to varying degrees) of a key management authority (usually the base station) post network deployment. In this paper, we presented an energy efficient security scheme for wireless sensor network which provides an end-to-end and inter node authentication for all communication in an efficient manner. The design of the security scheme is motivated by the observation that different types of messages exchanged between sensor nodes have different security requirements and that a single keying mechanism is not suitable for meeting these different security requirements. Consequently our scheme includes support for establishing two types of keys per sensor node individual keys which are shared with the base station, pair wise keys shared with individual neighboring nodes in the network. A distinguishing feature of our scheme is that it restricts the security impact of a node compromise to the immediate network neighborhood of the compromised node. The key establishment and key updating procedures for a compromised is used by our scheme.

REFERENCES

1. Akylidz, W. Su, Y. Sankarasubramaniam and E. Cayirci. Wireless Sensor Networks: A Survey. Computer Networks, March 2002.
2. Du W, Deng J, Han YS, Varshney PK. A pairwise key predistribution scheme for- Wireless Sensor Networks. In Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS-03), Washington D.C., October 2003.
3. Chorzempa M, Park JM, Eltoweissy M. SECK: survivable and efficient keying in Wireless Sensor Networks. IEEE Workshop on Information Assurance in Wireless Sensor Networks, WSNIA-2005, April 2005.
4. Eltoweissy M, Wadaa A, Olariu S, Wilson L. Group key management scheme for large-scale Wireless Sensor Network. Ad-Hoc Networks 2005.
5. Du W, Deng J, Han YS, Varshney PK. A pairwise key predistribution scheme for- Wireless Sensor Networks. In Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS-03), Washington D.C., October 2003.
6. Zhu S, Setia S, Jajodia S. LEAP: Efficient security mechanisms for large-scale distributed sensor networks. In Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS-03), Washington D.C., October 2003.
7. Jolly G, Kuscu M, Kokate P, Younis M. A low-energy key management protocol for Wireless Sensor Networks. In Proceedings of the IEEE Symposium on Computers and Communications (ISCC-03). Kemer-Antalya, Turkey. June 2003.
8. D. Liu, P. Ning, and W. Du. Group-Based Key Pre-Distribution in Wireless Sensor Networks, Proc. 2005 ACM Wksp. Wireless Security (WiSe 2005), Sept. 2005.
9. M. Younis, K. Ghumman, and M. Eltoweissy. Location aware Combinatorial Key Management Scheme for Clustered Sensor Networks, to appear, IEEE Trans. Parallel and Distrib. Sys., 2006.
10. Liu and P. Ning. Improving Key Pre-Distribution with Deployment Knowledge in Static Sensor Networks, ACM Trans. Sensor Networks, 2005.
11. L. Eschenauer and V. Gligor. A Key Management Scheme for Distributed Sensor Networks, Proc. 9th ACM Conf. Comp. and Commun. Sec., Nov. 2002.
12. J. Agre, L. Clare, An integrated architecture for cooperative sensing networks, IEEE Computer Magazine (May 2000).
13. N. Bulusu, D. Estrin, L. Girod, J. Heidemann, Scalable coordination for wireless sensor networks: self-configuring localization systems, International Symposium on Communication Theory and Applications, July 2001.
14. A. Cerpa, D. Estrin, ASCENT: adaptive self-configuring sensor networks topologies, UCLA Computer Science Department Technical Report, May 2001.
15. A. Chandrakasan, R. Amirtharajah, S. Cho, J. Goodman, G. Konduri, J. Kulik, W. Rabiner, A. Wang, Design considerations for distributed micro-sensor systems, Proceedings of the IEEE 1999 Custom Integrated Circuits.
16. Chien, I. Elgorriaga, C.McConaghy, Low-power directsequence spread-spectrum modem architecture for distributed wireless sensor networks, ISLPED'01, Huntington Beach, California, August 2001.
17. S. Cho, A. Chandrakasan, Energy-efficient protocols for low duty cycle wireless microsensor, Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, January 2000.
18. R. Colwell, Testimony of Dr. Rita Colwell, Director, National Science Foundation, Before the Basic Research Subcommitte, House Science Committe, Hearing on Remote Sensing as a Research and Management Tool, September 1998.

Anupriya Sharma, M.Tech(CS), B.Tech(CS) currently working as Asst. Prof at IIMT Engg. College Meerut presently working on WSN and published few papers on WSN in reputed International Journal.

Paramjeet Rawat, Ph.D(P), M.Tech(CS), MCA, currently working as Asst. Prof at IIMT Engg College Meerut having 12 years of Teaching Experience, member of ACM, published several papers in reputed International Journals.