International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-3 Issue-2, July 2013

A Pair Wise Key Pre-Distribution Scheme for Wireless Sensor Networks

Sowmya Lakshmi B S, Sowmya A N Gowda

Abstract— Wireless sensor networks (WSNs) are highly vulnerable to attacks for the limitation of constrained resource and communicating via wireless links, especially running in a hostile environment such as battlefields. In such situation, an adversary may capture any node compromising critical security data including keys used for confidentiality and authentication. Consequently, it is necessary to provide security services to these networks to ensure their survival. In this paper, we propose a new key management technique based on differentiated key pre-distribution, to provide end-to-end secure communication. The core idea is to distribute different number of keys to different sensors to enhance the resilience of certain links. This feature is leveraged during routing, where nodes route through those links with higher resilience. The analysis also shows that the technique can substantially improve the security as well as the performance of existing key pre-distribution techniques.

Index Terms— Sensor Networks, security, Key Management, Key Pre-distribution

I. INTRODUCTION

Wireless sensor networks consist of distributed, wirelessly enabled embedded devices capable of employing a variety of electronic sensors. A sensor node typically contains a power unit, a sensing unit, a processing unit, a storage unit, and a wireless transmitter / receiver. The microcontroller functions with the electronic sensors as well as the transceiver to form an efficient system for relaying small amounts of important data with minimal power consumption.

Wireless sensor networks are increasingly deployed in security-critical applications such as factory monitoring, environmental monitoring, burglar alarms and fire alarms. The sensor nodes for these applications are typically deployed in unsecured locations and are not made tamper-proof due to cost considerations. Hence, an adversary could undetectably take control of one or more sensor nodes and launch active attacks to subvert correct network operations. Such environments pose a particularly challenging set of constraints for the protocol designer: sensor network protocols must be highly energy efficient while being able to function securely in the presence of possible malicious nodes within the network.

Manuscript published on 30 July 2013.
***Correspondence Author(s)**
Sowmya Lakshmi B S, M.Tech Research Scholar, Department of Computer Science, Dayananda Sagar College of Engineering, Bangalore, India.
Sowmya A N Gowda, M.Tech Research Scholar, Department of Computer Science, Dayananda Sagar College of Engineering, Bangalore, India.

A. Routing Protocol in WSNs

The primary functionality of wireless sensor networks is to sense the environment and transmit the acquired information to base stations for further processing. Thus, routing is an essential operation in sensor networks.

Routing in wireless sensor networks has some differences from that in traditional wired and wireless ad hoc networks due to resource constraints, faults/failures etc. There are two main paradigms of routing protocols in WSNs: location-centric routing and data-centric routing.

1) Location-centric routing: Greedy Perimeter Stateless Routing (GPSR) is a well known location centric routing protocol. In GPSR, beacon messages are broadcast by each node to inform its neighbors of its position. GPSR assumes that sensors can determine through separate means the location of the sink. Each node makes forwarding decisions based on the relative position of the sink and its neighbors. In general, the neighbor that is closest to the sink is chosen.

2) Data-centric routing: Directed diffusion is the most well known data centric routing protocol, in which the sink sends queries to all nodes and waits for data from the nodes satisfying specific requirement (e.g., located in selected regions, sensing data meet certain criteria, etc). In order to create a query, an interest is defined using a list of attribute-value pairs such as name of objects, geographical area, etc. The interest is broadcast through the network, and used by each node to compare with the data received. The interest entry also contains several gradient fields. A gradient is a reply link to a neighbor from which the interest was received. By utilizing interests and gradients, paths are established between sensors and the sink. Several paths may be established, and one of them is selected by reinforcement.

B. Key Management Schemes in Sensor Networks

To achieve security in wireless sensor networks, it is important to be able to perform various cryptographic operations, including encryption, authentication, and so on. Keys for these cryptographic operations must be set up by communicating nodes before they can exchange information securely. Key management schemes are mechanisms used to establish and distribute various kinds of cryptographic keys in the network, such as individual keys, pairwise keys, and group keys. Key management is an essential cryptographic primitive upon which other security primitives are built. Most security requirements, such as privacy, authenticity, and integrity, can be addressed by building on a solid key management framework. In fact, a secure key management scheme is the prerequisite for the security of these primitives, and thus essential to achieving secure infrastructure in sensor networks. Due to resource constraints, achieving such key agreement in wireless sensor networks is nontrivial.

The challenge of designing key management protocols for sensor networks lies in establishing a secure communication infrastructure, before any routing fabric has been established with or without the presence of any trusted authority or fixed server, from a collection of sensor nodes that have no prior contact with each other. Some cryptographic information (e.g., a key) is normally preloaded in sensor nodes before deployment, and allows sensor nodes to perform secure communications with each other. Most schemes do not assume prior knowledge of the network deployment topology and allow nodes to be added to the network after deployment. The schemes must have low computational and low storage requirements. There are three types of general key management schemes: trusted-server scheme, self-enforcing scheme, and key pre-distribution scheme. The trusted-server scheme depends on a trusted server for key agreement between nodes, e.g., Kerberos. This type of scheme is not suitable for sensor networks because there is no trusted infrastructure in sensor networks. The self-enforcing scheme depends on asymmetric cryptography, such as key agreement using public key certificates. However, limited computation and energy resources of sensor nodes often make it undesirable to use public key algorithms, such as Diffie-Hellman key agreement or RSA. The third type of key agreement scheme is key pre-distribution, where key information is distributed among all sensor nodes prior to deployment. If we know which nodes will be in the same neighborhood before deployment, keys can be decided a priori. However, most sensor network deployments are random; thus, such a priori knowledge does not exist. Key pre-distribution offers two inadequate solutions: either a single mission key or a set of separate n-1 keys, each being pair-wise privately shared with another node, must be installed in every sensor node. The single mission-key solution is inadequate because the capture of any sensor node may compromise the entire WSN since selective key revocation is impossible upon sensor capture detection. In contrast, the pair-wise private sharing of keys between every two sensor nodes avoids wholesale WSN compromise upon node capture since selective key revocation become possible. However, this solution requires pre-distribution and storage of $n-1$ keys in each sensor node, and $n(n-1)/2$ per WSN, which renders it impractical for WSNs using, say, more than 10,000 nodes, for both intrinsic and technological reasons. First, pair-wise private key sharing between any two sensor nodes would be unusable since direct node-to-node communication is achievable only in small node neighborhoods delimited by communication range and sensor density. Second, incremental addition and deletion as well as re-keying of sensor nodes would become both expensive and complex as they would require multiple keying messages to be broadcast network-wide to all nodes during their non-sleep periods (i.e., one broadcast message for every added/deleted node or re-key operation). Third, a dedicated RAM memory for storing $n-1$ keys would push the on-chip, sensor-memory limits for the foreseeable future, even if only short, 64-bit, keys are used 1 and would complicate fast key erasure upon detection of physical sensor tampering. In order to provide secure communications between neighboring nodes in randomly deployed WSNs, Random key pre distribution (RKP) was proposed [1]. In its basic version, each sensor is pre-distributed with k distinct keys randomly chosen from a large pool of K keys. After deployment, neighboring nodes use these pre-distributed keys to establish a pair wise key between them. Communications between neighboring sensors in each hop are encrypted/decrypted using these pair wise keys. The resilience of each hop (link) can be reflected by the number of shared pre-distributed keys in the link. It is known that under uniform key distribution, i.e. each sensor pre distributed with equal number of keys, will achieve maximum average number of shared pre-distributed keys in each link. However, there is an inherent limitation in uniform key distribution.

- Majority of links have small number of shared keys. Hence low resilience
- The percentage of links that are highly resilient is quite low
- Restricts the room for routing protocols to choose more resilient links during end to end communications.
- Installing more keys into each node is not always preferable since it enables the attacker to disclose more keys upon node captures, which could again compromise the link resilience.

Our approach: We propose a simple key pre-distribution scheme that requires memory storage for only few tens to a couple of hundred keys, and yet has superior security and operational properties when compared to those of uniform key distribution. For end to secure communications in randomly deployed WSNs we propose a methodology called differentiated key predistribution. The methodology of our protocol is to predistribute different number of keys to different nodes. By distributing more keys to some nodes, the links between those nodes tend to have much higher resilience than the link resilience under uniform key pre-distribution. To enhance the end to end secure communications links with high resilience are given preference compared with links with low resilience during routing to the sink node. For fairness in analysis, the average number of keys per node in our scheme is kept same as that in uniform key pre-distribution. Assuming that the probability of node capture is the same for all nodes, the attack impact (i.e., expected number of unique keys disclosed under node capturing attack) remains the same in both uniform and our heterogeneous key distribution scheme, making performance comparisons fair.

II. RELATED WORKS

The literature survey carried out has revealed that a fair amount of research has been put in the areas of wireless sensor networks. B. Karp et., al [1] has proposed Greedy Perimeter Stateless Routing (GPSR), a novel routing protocol for wireless datagram networks that uses the positions of routers and a packet's destination to make packet forwarding decisions. GPSR makes greedy forwarding decisions using only information about a router's immediate neighbors in the network topology.C. Intanagonviwat, et., al [2] have proposed a directed diffusion paradigm for such coordination. Directed diffusion is data centric in that all communication is for named data. All nodes in directed diffusion-based network are application aware./this enables diffusion to achieve energy savings by selecting empirically good paths and by caching and processing data in-network. Heinzelman, et., al [3] has proposed LEACH

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

(Low-Energy Adaptive Clustering Hierarchy), a clustering-based protocol that utilizes randomized rotation of local cluster base stations (cluster-heads) to evenly distribute the energy load among the sensors in the network. LEACH uses localized coordination to enable scalability and robustness for dynamic networks, and incorporates data fusion into the routing protocol to reduce the amount of information that must be transmitted to the base station. C. Schugers, et., al [4] has proposed new scheme for the purpose of routing in the wireless sensor networks. The proposed approach is for the case in which many sensors need to collect data and send it to a central node. In order to find the routes that give energy efficiency, a set of partial differential equations similar to the Maxwell's equations in the electrostatic theory are solved. Laurent Eschenauer, et., al [5] have proposed a key-management scheme designed to satisfy both operational and security requirements of DSNs. The scheme includes selective distribution and revocation of keys to sensor nodes as well as node re-keying without substantial computation and communication capabilities. It relies on probabilistic key sharing among the nodes of a random graph and uses simple proto cols for shared-key discovery and path-key establishment, and for key revocation, re-keying, and incremental addition of nodes. In order to overcome the resilience of the basic key management protocol in [5], in [6] and [7], multiple key paths are used to enhance resilience of the link between two nodes. However, exploiting high resilience key paths for routing is not discussed. In [8] and [10], each sensor is pre-distributed with k key structures (vectors or polynomials) from a key structure pool, where each key structure has degree λ. In such schemes, no key structure is disclosed until at least λ+1 nodes pre-distributed with this key structure are captured. When λ = 0, this scheme degrades to the basic *RKP* scheme. S. Tanachaiwiwat, et., al [9] have proposed the novel concept of secure locations to address non-cooperative and malicious behavior in location-aware sensor networks. Architecture also introduces as scalable trust-based routing protocol (TRANS) to track, update and route around untrusted locations using variants of geographic and trajectory routing. Protocol provides an efficient algorithm for identifying and isolating misbehaving or compromised sensors based on their approximate locations.

In the recent past, there have been a host of orthogonal dimensions where random key pre-distribution has been adapted in sensor networks. While works in [11] and[15] use deployment knowledge (i.e., partial knowledge of sensor locations in the network) to enhance pair-wise key set-up among nodes. In [12]SIGF (Secure Implicit Geographic Forwarding) is proposed, a configurable secure routing protocol family for wireless sensor networks that provides \good enough" security and high performance. By avoiding or limiting shared state, the protocols prevent many common attacks against routing, and contain others to the local neighborhood. P. Traynor, et., al [13] has proposed a probabilistic unbalanced distribution of keys throughout the network that leverages the existence of a small percentage of more capable sensor nodes can not only provide an equal level of security but also reduce the consequences of node compromise. We demonstrate the effectiveness of this approach on small networks using a variety of trust models and then demonstrate the application of this method to very large systems. S. Chellappan, W. Gu, et., al [14] has proposed two methodologies. First algorithm is called the Optimal Maximum Flow based centralized (OMF) algorithm. An alternate algorithm called the Domain-based OMF (D-OMF) algorithm extending from the OMF algorithm that trades optimality with computational complexity and messaging overhead. Finally, the Simple Pit-Peak based distributed (SPP) algorithm that uses local requests and responses for sensor movements is proposed. A. Poornima et., al [16] has proposed two key management schemes for hierarchical networks which handles various events like node addition, node compromise and key refresh at regular intervals. In [17] triangle-based key predistribution has been proposed, This is achieved by using the bivariate polynomial in a triangle deployment system based on deployment information about expected locations of the sensor nodes. Y. Lee et., al [18] Wireless Sensor and Actor Networks (WSANs) with immediate-response actor nodes have been proposed which adds greater mobility and activity to the existing sensor networks. This research seeks to demonstrate ways to provide security, integrity, and authentication services for WSAN's secure operation, by separating networks into hierarchical structure by each node's abilities and provides different encryption key-based secure protocols for each level of hierarchy: Pair-wise key, node key, and region key for sensor levels, and public key for actor. N. Canh, et., al [19] has proposed a practical deployment model, where sensor nodes are deployed in groups, and the nodes in the same group are close to each other after the deployment. In [20] Differentiated key pre-distribution is proposed. The core idea is to distribute different number of keys to different sensors to enhance the resilience of certain links. This feature is leveraged during routing, where nodes route through those links with higher resilience.

III. METHODOLOGY

In order to provide a high quality of end to end secure communications, it is clear that we should enhance the resilience of individual links in the network. Resilience is the probability that a pairwise key (link) between two nodes is not compromised under attack. An efficient way to do so is to increase the number of keys pre-distributed into each node (k). When the number of shared keys in each link increases, resilience seems to increase since all shared keys have to be disclosed to compromise the link.

A methodology called differentiated key distribution is proposed to provide end to end secure communication between nodes and sink in randomly deployed WSNs. The basic idea of our methodology is to pre-distribute different number of keys to different nodes. Our methodology is based on the observation that links in the network are not equally important with respect to secure communications. Only the links used for data transmission have impacts on security.

In our scheme, key distribution consists of two phases, namely key pre-distribution, pair-wise key establishment.

Protocol Parameter.

Notations	Protocol Parameter
S	Network area(=πR^2)
r	Communication range
N	Number of nodes in network
c	Number of nodes classes

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

n_i	Number of class i nodes($1 \le i \le c$)
k_i	Number of key pre-distribution in class i node($1 \le i \le c$)
K	Number of keys in key pool

Table 1. Protocol Parameter.

A. *Key pre-distribution*

In this framework a network of N sensor nodes and a sink node is considered. N sensor nodes are divided into c classes, each of which has $n_i (1 \le i \le c)$ nodes. We call the sensors in the i^{th} class as class i nodes. Class c being the least powerful nodes, and Class 1 the most powerful nodes, in terms of the keys distributed to the nodes of each class. We then pre-distribute k_i ($1 \le i \le c$ and $k1 \ge k2 \ge \cdots \ge kc$) unique keys chosen from a large key pool with size K into each class i node. The sink node is pre-distributed with all K keys in the key pool and is deployed strategically at certain position, while the N sensor nodes are deployed randomly in the network.

For each class 1 node, its k1 unique keys are chosen randomly from the key pool. Keys to the other class nodes are distributed in semi random way from class 1 to increase the chance of key sharing between other class nodes and class 1 nodes. For a Node in class i (i > 1), class 1 nodes are randomly divided into type A and type B. Type A consists of $n1 - (ki - \lfloor ki/n1 \rfloor \cdot n1)$ class 1 nodes. Type B consist of $ki - \lfloor ki/n1 \rfloor \cdot n1$ class 1 nodes. For a node in class i , $\lfloor ki/n1 \rfloor$ keys are first chosen randomly from the distributed keys in each type A nodes, for the remaining type B nodes $\lfloor ki/n1 \rfloor$ keys are chosen randomly from the distributed keys of each node. By distributing keys in this way, we guarantee ki unique keys are distributed, and the number of keys chosen from each class 1 node are balanced and differs by at most 1. The reason we pre-distribute keys for class i nodes in the above semi random way instead of purely randomly is two folded. First, we can enhance the probability that a class i node shares key with a class 1 node. Second, we do not decrease the probability that a class i node shares key with a non-class 1 node.

B. *Pair-wise key establishment*

Once nodes are pre distributed with keys and deployed, they start to discover their neighbors within their communication range r via local communication, and obtain the key IDs of their neighbors' pre-distributed keys. With the above information each node in the framework performs two steps to establish pair-wise keys between its neighbor nodes: (a) direct key setup (one hop key path), and (b) path key setup (two hop key path) . The direct key setup step is for any two nodes trying to establish a pair-wise key; and they always first attempt to do so through direct key establishment in a peer-to-peer manner. Each sensor node also start path key setup step with all its neighbors, trying to establish a pair wise key with the help of other sensors. After a node i construct all two hop key paths to node j, node i will generate multiple random key shares, and transmit each key share on each key path. Key shares are encrypted /decrypted hop by hop by a combination (e.g., XOR) of all shared keys on that hop. Ultimately, the pair-wise key between nodes i and j is a combination of all the key shares (e.g, XOR) transmitted.

IV. PERFORMANCE EVALUATION

Use evaluation is focused on following standard metrics:

a) *Connectivity*: Connectivity is the probability that two physical neighbors can establish a pair wise key between them.

b) *Resilience*: Resilience is the probability that a pairwise key (link) between two nodes is not compromised under attack.

A) *Simulation setup*

We conduct our simulation using a NS2 simulator. The network is circular with radius 500 *meters*, where N=100 nodes are uniformly deployed at random. The sink is at the center of the network. The network parameters assumed are: $c = 2$, $n1 = 20$, $n2 = 80$, $k1 = 80$, $k2 = 30$, $K = 1000$, $r = 100$ *meters* (for notation, please refer to Table 1 in Section 3). Our communication model is one where sensors periodically transmit data to the sink. Routing protocol used is For uniform key pre-distribution model each node is pre-distributed with 20 keys. The network animator output for 100 nodes with 10 malicious nodes indicated in red circle is shown in Figure 1.

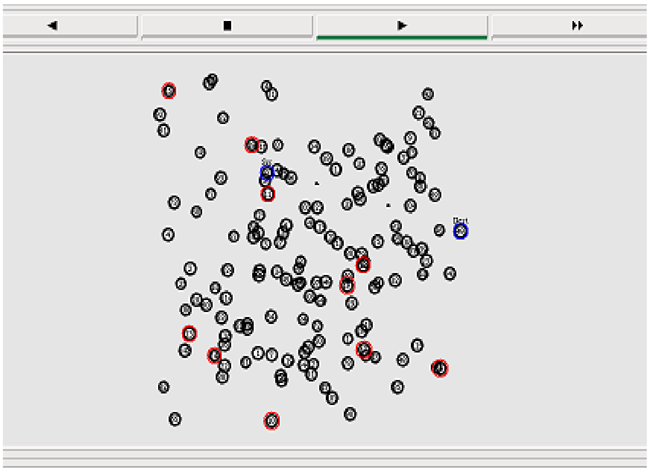

Figure 1..Network animator output for 100 nodes with 10 malicious nodes.

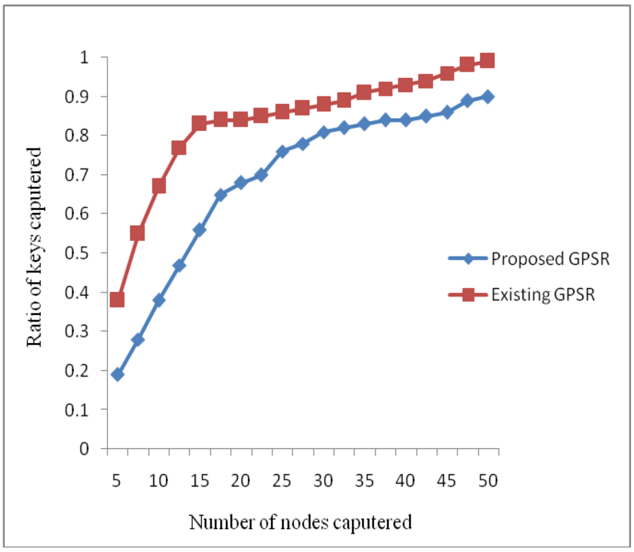

Figure 2. Expected ratio of keys captured vs. number of nodes captured.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

In Figure 2, the expected ratio of keys captured is plotted as a function of the number of nodes captured for several instances of GPSR protocol with uniform key pre-distribution(Existing GPSR) and GPSR protocol with differentiated key distribution(Proposed GPSR).

V. CONCLUSION

We presented a new key management technique for randomly deployed wireless sensor networks. Our proposed solution improves considerably resilience to links compromising compared with other protocols. Where the idea is to distribute different number of keys to different sensors to enhance the resilience of certain links in the network. We present our end to end secure communication protocol based on the above methodology by well known location centric (GPSR) routing protocol. The technique is analyzed in detail with respect to link resilience for node capture attacks. Analysis shows that our technique exhibits better performance against node capture attacks.

REFERENCES

1. B. Karp and H. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in Proc. ACM International Conf. Mobile Compute. Netw., Aug. 2000.
2. C. Intanagonviwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in Proc. ACM International Conf. Mobile Comput. Netw., Aug. 2000.
3. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan," Energy efficient communication protocols for wireless micro sensor networks (leach)", Proceedings of the 33rd Hawaii International Conference on System Sciences - 2000.
4. C. Schugers and M. Srivastava, "Energy efficient routing in wireless sensor networks," in Proc. Milcom, Oct. 2001.
5. L. Eschenauer and V. D. Gligor, "L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for distributed sensor networks," in Proc. 9th ACM Conf. Comput. Commun. Security, Nov. 2002.
6. H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proc. IEEE Symp. Research Security Privacy, May 2003.
7. S. Zhu, S. Xu, S. Setia, and S. Jajodia, "Establishing pairwise keys for secure communication in ad hoc networks: a probabilistic approach," in Proc. 11th IEEE International Conf. Netw. Protocols, Nov. 2003.
8. D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in Proc. 10th ACM Conf. Comput. Commun. Security, Oct. 2003.
9. S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy, "Secure locations: routing on trust and isolating compromised sensors in location aware sensor networks," in Proc. 1st ACM Conf. Embedded Netw. Sensor Syst., Nov. 2003
10. W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," in Proc. 10th ACM Conf. Comput. Commun. Security, Oct. 2003.
11. D. Liu and P. Ning, "Improving key predistribution with deployment knowledge in static sensor networks," ACM Trans. Sensor Netw., vol. 1, no. 2, pp. 204-239, 2005.
12. A. D. Wood, L. Fang, J. A. Stankovic, and T. He, "SIGF: a family of configurable, secure routing protocols for wireless sensor networks," in Proc. 4th ACM Workshop Security Ad Hoc Sensor Netw., Oct. 2006.
13. P. Traynor, H. Choi, G. Cao, S. Zhu, and T. L. Porta, "Establishing pair-wise keys in heterogeneous sensor networks," in Proc. 25th IEEE Conf. Comput. Commun., Apr. 2006.
14. S. Chellappan, W. Gu, X. Bai, B. Ma, D. Xuan, and K.Zhang, "Deploying wireless sensor networks under limited mobility constraints," IEEE Trans. Mobile Comput., vol. 6, no. 10, Oct. 2007.
15. D. Liu, P. Ning, and W. Du, "Group-based key predistribution for wireless sensor networks," ACM Trans. Sensor Netw., vol. 4, no. 2, pp. 1-30, 2008.
16. A. Poornima and B. Amberker," Key Management Schemes for Secure Communication in Heterogeneous Sensor Networks", International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009.
17. H. Dai and H. Xu, "Triangle-based key management scheme for wireless sensor networks," Frontiers Electrical Electron. Eng. China, vol. 4, no. 3, pp. 300-306, 2009.
18. Y. Lee and S. Lee," A new efficient key management protocol for wireless sensor and actor networks", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 2, 2009.
19. N. Canh, P. Truc, T. Hai, Y. Lee, and S. Lee, "Enhanced group-based key management scheme for wireless sensor networks using deployment knowledge," in Proc. 6th IEEE Consumer Commun. Netw. Conf., pp. 1- 5, 2009.
20. Wenjun Gu, Neelanjana Dutta, Sriram Chellappan, And Xiaole Bai," Providing End-To-End Secure Communications In Wireless Sensor Networks", IEEE Transactions On Network And Service Management, Vol. 8, No. 3, September 2011.

AUTHOR PROFILE

Sowmya Lakshmi B S has received B.E degree in 2011 from VTU, Belgaum, Karnataka, India. Currently she is pursuing M.Tech in VTU. Her areas of interests include wireless sensor networks.

Sowmya A N Gowda has received B.E degree in 2011 from VTU, Belgaum, Karnataka, India. Currently she is pursuing M.Tech in VTU. Her areas of interests include wireless sensor networks.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)