Secure Routing in Wireless Sensor Networks

Mrs Soumyashree Sahoo [1], Mr Pradipta Kumar Mishra [2] and Prof.Dr.Rabi Narayan Satpathy[3]

[1]**Department of Computer Science and Engineering, Biju Patnaik University of Technology, Hi-Tech Institute of Technology**
Bhubaneswar, Orissa 752055/7, India

[2] **Department of Computer Science and Engineering , Biju Patnaik University of Technology, Hi-Tech Institute of Technology**
Bhubaneswar, Orissa 752055/7, India

[3] **Department of Computer Science and Engineering , Biju Patnaik University of Technology, Hi-Tech Institute of Technology**
Bhubaneswar, Orissa 752055/7, India

Abstract

Wireless sensor networks is the new concept in the field of networks consists of small, large number of sensing nodes which is having the sensing, computational and transmission power. Due to lack of tamper-resistant infrastructure and the insecure nature of wireless communication channels, these networks are vulnerable to internal and external attacks. Key Management is a major challenge to achieve security in wireless sensor networks. Key management includes the process of key setup, the initial distribution of keys and keys revocation. To provide security and proper routing or communication should be encrypted and authenticated. It is not easy to achieve secure key establishment without public key cryptography. In this thesis, some key management schemes have been purposed which will be valuable for secure routing between different sensor nodes.

Keywords: Security, Design, Sensor networks, Key management, Algorithms

1. Introduction

Wireless sensor networks consist of spatially distributed sensors to co-operatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants. When sensor networks are deployed in a hostile environment, security becomes extremely important, as they are prone to different types of malicious attacks. For example, an adversary can easily listen to the traffic, impersonate one of the network nodes, or intentionally provide misleading information to other nodes. The flexibility, fault tolerance, high sensing fidelity, low-cost and rapid deployment characteristics of sensor networks create many new and exciting application areas for remote sensing.

Key Management includes the processes of key setup, the initial distribution of keys and key revocation. To provide security and communication should be encrypted and authenticated. The open problem is how to bootstrap secure communications between sensor nodes, i.e. how to set up secret keys between communicating nodes. This problem is known as the key agreement problem. There are three types of general key agreement schemes: trusted-server scheme, self-enforcing scheme, and key pre-distribution scheme. The trusted-server scheme is not suitable for sensor networks because there is no trusted infrastructure in sensor networks. The self-enforcing scheme that depends on asymmetric cryptography is inapplicable for using public-key algorithms due to limited computation and energy resources of sensor nodes. 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 neighbourhood before deployment, keys can be decided a priori. However, most sensor network deployments are random; thus, such a priori knowledge does not exist. Thus, we have to make tradeoffs between security and the available resources while designing an

efficient key management scheme to achieve better security. The key management schemes must establish a key between all sensor nodes that must exchange data securely, node addition or deletion should be supported, Security services such as authentication and key management are critical to secure the communication between sensors in hostile environments. The key management schemes that we are going to present, must establish a key between all sensor nodes that must exchange data securely, node addition or deletion should be supported, It should work in undefined deployment environment, unauthorized nodes should not be allowed to establish communication with network nodes. The proposed key management protocols have been presented in detail.

1. When a sensor node wants to communicate with another sensor node, they need to be authenticated with each other first. Motivated by this, we proposed an Authentication Scheme without storing direct key information in the memory of individual sensor nodes.
2. Two communicating nodes need to have a pair wise key for secure communication. We proposed a pair wise key establishment scheme by using a counter.
3. Compromised nodes could deviate the network behaviour by injecting false data or modifying data of correct nodes. Thus, compromised nodes should not be taking part in the group communication. To solve this problem we proposed the key management scheme for node revocation.

2. Related Work

All key management schemes can be categorized in to two types i.e. pre-distribution key management schemes where key information is distributed among all sensor nodes prior to deployment and in Insitu key management schemes which does not require keying information prior to deployment .This key pre-distribution can be divided into several categories based on Key Pool, Random Pair Wise Key, Key Space, Group, grid-based etc. In key pool based scheme, a large key pool is computed offline and each sensor is preloaded with keys Selected randomly without replacement from the key pool. These keys form a sensor's key ring. Laurent Eschenauer and Virgil D. Gligor proposed a probabilistic key pre distribution scheme[2]. The main idea was to let each sensor node randomly pick a set of keys from a key pool before deployment so any two-sensor nodes sharing at least one common key. Donggang Liu and Peng Ning [9] presented a key management scheme where sensors can be added dynamically without having to contact the previously deployed sensors. This scheme allows the network to grow. In 2003 Chan et al proposed the Random pair wise scheme [3]. The random pair wise scheme possesses perfect resilience against node capture attacks as well as support for node based revocation and resistance to node replication. In 2009 Stephen Anokye et al [6] made improvements on Chan et al's Random pair wise scheme. This scheme significantly reduces the memory and computational overheads and it has better connectivity. In that year Du et al proposed a pair wise key predistribution scheme that is scalable and flexible. It is substantially more resilient against node capture. In 2005 Zhen Yu and Yong Guan proposed a group based key pre distribution scheme [11] using sensor deployment knowledge where a sensor field is partitioned into hexagonal grids. It consists of a series of methods depending on how to distribute secret information among neighbouring groups and how much information to be stored in each node which achieves a higher degree of connectivity of the sensor network with a lower memory requirement and offers a stronger resilience against node capture attacks. In 2006 R. Kalindi et al proposed a Grid based Key Pre-Distribution Scheme [12] for Distributed Sensor Networks that uses multiple mappings of keys to nodes. In each mapping, every node gets distinct set of keys, which it shares, with different nodes. The key assignment is done such that, there will be keys in common between nodes in different sub-grids. After randomly being deployed, the nodes discover common keys, authenticate and communicate securely. This scheme is able to achieve better security. Being motivated by the above key management schemes, some protocols have been developed for solving some of the important security issues that are encountered in Wireless sensor networks.

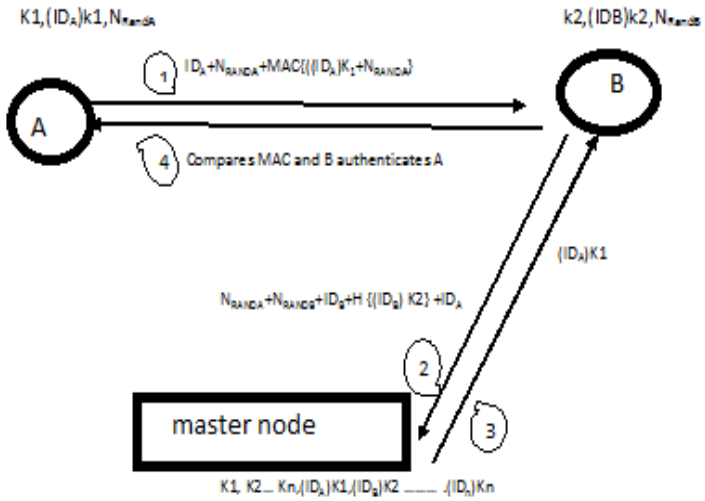
3. Proposed Key Management Schemes

Conventional key exchange and key distribution protocols based on infrastructures using trusted third parties are impractical for large-scale sensor networks because of the unknown network topology prior to deployment, communication range limitations, intermittent sensor-node operation, and network dynamics. To date, the only practical options for the distribution of keys to sensor nodes of large-scale distributed sensor networks whose physical topology is unknown prior to deployment would have to rely on key pre distribution. Keys would have to be installed in sensor nodes to accommodate secure connectivity between nodes. Security services such as authentication and key management are critical to secure the communication between sensors in hostile environments. Here three schemes have been proposed i.e. authentication, pair wise key establishment and a scheme for node revocation in an existing sensor network. The proposed key management schemes are presented in detail.

3.1 Authentication Scheme between two Individual Sensor Nodes:

When a sensor node wants to communicate with another sensor node, they need to be authenticated with each other first. In this scheme, it is assumed that no key information will be stored in individual sensor nodes; instead, every key information will be stored at a high-end sensor node i.e. the master node. By protecting only that master node, we can make the entire sensor network secure. The scheme is shown through an algorithm explained below.

1. Assuming the case of sensor node A and sensor node B in the network wants to securely communicate with each other.
2. The master node must contain keys of all sensor nodes i.e. K1, K2, K3... Kn and id's of all sensor nodes and encrypted form of there ids with their corresponding key i.e. (ID_A) K1,(ID_B)K2, (ID_C)K3,…… prior to deployment. The key is only available with the master node. Here sensor node A contains ID_A and (ID_A)K1 and sensor node B contains ID_B and (ID_B)K2 .
3. Sensor node A generates a random number i.e. Nonce A and computes the MAC using (ID_A)K1 and Nonce A .
4. Subsequently node A sends a message i.e. IDA||NonceA|| MAC {(IDA)K1|| Nonce A} to sensor node B.
5. Upon receiving the message, Node B tries to calculate the MAC for authentication. But as the key is only available with the master node so, sensor node B generates a random number i.e. Nonce B after getting the message from sensor node A and sends a message i.e. NonceA||NonceB|| ID_B ||H{(ID_B)K2}|| ID_A to the master node to verify the identity of sensor node A.
6. Master node recognizes IDB and then authenticate by computing the hash over the {(IDB)K2 }which is with the master node. After authenticating node B from the message received from sensor node B and becomes sure about the validity of the message and confirm about the validity of sensor node A by sending (IDA)K1 to sensor node B.
7. Sensor node B then computes MAC {(IDA)K1|| Nonce A} and compares it with the MAC present in the message coming from sensor node A . If those two MACs match with each other then it becomes sure that Sensor node A is a valid node in the network and communication with it is safe.



FigCaption1: Authentication Procedure

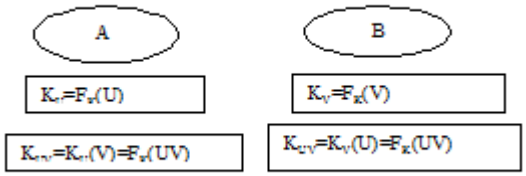
While node B communicating with the master node, if any adversary takes away all the communicated data ,it would be of no use as the (IDB)K2 of node B at node B had already been changed to (IDB)K2+ N_{RANDA} , and similarly at the master node the change to the (IDB)K2 to(IDB)K2+ NonceA also takes place. So the data communicated between node B and master node if intercepted is of no use. Once master node authenticate node B the master node can directly send the Nonce B to node A .So that node A can update (IDA)K1 to (IDA)K1+NonceB and the same updation is also being carried out by the master node. Thus authentication between two sensor nodes is performed in the proposed scheme. Authentication is done solely by the master node.

3.2 Pair-Wise Key Establishment among two individual Sensor Node

In the pair wise techniques, generally a key used to establish a secure channel between a couple of nodes, where no one can use this channel to perform any type of communication without of the permission of the owner node of the key itself.

1. Let us consider there are two nodes having id U and V, want to communicate with each other. The node U computes its key K_U as $K_U = F_K(U)$ .Here F_K is a function and the node id U is an input to the function. Similarly the node V computes its key K_V as $K_V = F_K(V)$.
2. Node U computes its pair wise key $K_{UV} = K_U (V) = F_K(UV)$ and node V computes its pair wise key $K_{UV} = K_V (U) = F_K (UV)$.
3. After the establishment of the pair wise key they start to transmit message to each other. Any message M is encrypted as $M= K_{UV}(M)$. A counter is set to keep records of transmitted message. With each transmission the

counter value is incremented at both the ends, so that the same message get encrypted differently each time which creates confusion for the attacker to decipher the key, as the key keeps changing with each transmission.



FigCaption2: Pair wise key establishment mechanism

4. After transmission of one message, the counter value is changed to some value C and the pair wise key between the sensor nodes becomes updated by that value i.e. $K_{UV} = F_K(UV+C)$. A message M can be encrypted as $M= K_{UV}(M) = F_K(UV+C)(M)$.

The main task of this scheme is to minimize the used memory for storing the different keys of the WSN, in addition to generating a strong and robust environment against any possible attack, and in case of any attack, the scheme should be flexible and fast in recovering.

3.3 Key management scheme for node revocation in the network

As the sensor nodes deployed in a network has the different limitations, hence in turn they get malicious or compromised and they hamper secure communication in the network by incorporating incorrect information or modifying data at other nodes in the network. This leads to the origination of an idea of assuming a private symmetric key called group key, which is used to transfer the messages within the group. When a compromised node is found, the current group key must be cancelled or revoked and a new key must be provided to all the group members except the compromised or malicious node. Hence it leads to the removal of the compromised Sensor node.

The protocol is efficient and scalable as it limits both communication and computation overhead during rekeying. This scheme follows an approach of node management (NM) that cancels the current group key and distributes a new group key to all the nodes except the compromised one and in turn forces the compromised nodes to leave the group.

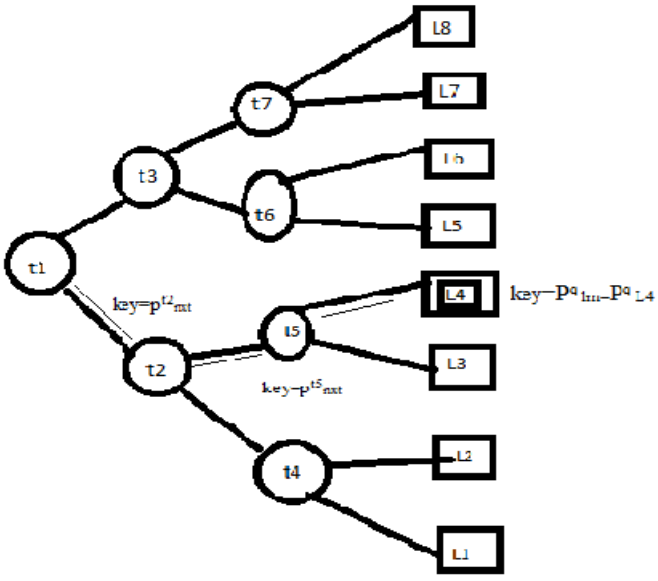
The node revocation procedure lies on the concept of group key set up phase, where a sender(G) wants to communicate with the receiver node(H) .In the key set up phase G creates a key-set, a sequence of values $< P_0 . . . P_i . . . P_N >$, where each key is linked to other ones by means of a hash function H. G randomly chooses the end-key P_N and then iteratively applies the one-way function H for N times in order to obtain the start-key at the beginning of the chain. That is,

$$P_i = H(P_{i+1}), \quad (0 \leq i < N)$$

Each key in the set (except the start-key) is the hash preimage of the previous one in the direction of the start key. That is, the key P_i is the hash preimage of P_{i+1} .

The node revocation scheme is explained in the following steps.

1. Assume that each sensor node shares a secret symmetric key that shares with NM and is denoted by P^q_{ln} i.e.; the key of the sensor node l_n.
2. To remove a malicious node l_m, NM maintains a stepwise structure of symmetric keys, called **the node-revocation tree.**
3. NM associates each internal node t_a of the node revocation tree with a chain composed of N_{ta} keys and each leaf node with the secret key of a group member. Initially, the current-key of the internal node t_a , $P^{ta}_{cur,}$ corresponds to the start-key, P^{ta}_0.Thus, in the setup phase current keys contains only the start-keys.
4. A sensor node l_n stores a set of current keys, key ring(l_n) can be defined as, $KeyRing(ln) = \{P^{ta}_{cur} \mid ta \in Path(l_n)\}$, where Path($l_n$) be the set of internal nodes lying on the path from the root to the leaf associated with l_n. The key-set KeyRing(l_n) is composed of the current-keys associated with the internal nodes in Path (l_n).
5. Every group member stores a copy of the current-key associated with the tree root, P^{t1}_{cur}, because it belongs to the key-set of every group member. Thus, this key acts as the group-key.
6. When a sensor node l_m is compromised and NM has to renew them, but it isn't renewed for l_m.



FigCaption3: Node revocation scheme

7. For each internal node t_a in Path(l_m), and for each child of t_a, NM broadcasts a rekeying message structured as follows. Every message contains the next-key of t_a, P^{ta}_{nxt}. If the t_a 's child is a leaf and it is not associated with P^{q}_{lm}, P^{ta}_{nxt} is encrypted with the private-key of the corresponding group member. If the t_a's child is an internal node (i,e; t_c) and is not included in Path(l_m), P^{ta}_{nxt} is encrypted with P^{tc}_{cur}. If t_c is included in Path(l_m), P^{ta}_{nxt} is encrypted with P^{tc}_{nxt}.
8. After this procedure, for each internal node ta belonging to path l_m, P^{ta}_{cur} is replaced by P^{ta}_{nxt}. Hence the leaf node with P^{q}_{lm} is removed by the NM.

4. Conclusion

Security is the major concern in the wireless sensor networks. The communication of information between the sensor nodes gets tampered due to the malicious behaviour of the network. Hence in this paper, three schemes are discussed for secure routing between the sensor nodes using the concept of key management. The authentication scheme maintains an efficient and secure communication between two different nodes. The pair-wise key management scheme enforces security in terms of one private paired key. The third scheme explains one scheme for the problem of insecure behaviour of a compromised node, where the compromised node is revoked from the group to make the network more secure, efficient and scalable.

References

[1] D.Estrin, R.Govindan, J.Heidemann, and S.Kumar, Next century challenges: scalable coordination in sensor networks, ACM MobiCom'99, Washington, USA, 1999, pp. 263–270.
[2] Laurent Eschenauer and Virgil D.Gligour.A Key Management Scheme for Distributed Sensor Networks. In proceedings of the 9th ACM conference on Computer and Communication Security, Pages 41-47, November 2002.
[3] H.chan, A.Perrig and D.Song, Random Key Predistribution Schemes for Sensor Networks. In IEEE Symposium on Security and Privacy, pages 197213, Berkeley, California, May 11-14, 2003.
[4] Pair wise Key Management Scheme Using Sub Key Pool for Wireless Sensor Networks by Jianmin Zhang, Yu Ding of Henan Institute of Engineering, China 2010 Second International Conference on Information Technology and Computer Science.
[5] A Promising Pair wise Key Establishment Scheme for Wireless Sensor Networks in Hostile Environments by WenqiYu of Henan Institute of Engineering, China.
[6] Stephen Anokye, Thabo Semong, Qiaoliang Li, Qiang Hu ,"Group wise Pair wise Scheme for Wireless Sensor Networks," niss, pp.695-699, 2009 International Conference on New Trends in Information and Service Science, 2009
[7]A Pair wise Key Establishment for Wireless Sensor Networks Found in: 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing By Hung-Min Sun, Yue-Hsun Lin ,Cheng-Ta Yang , Mu-En Wu
[8] A new pair wise key establishment scheme for sensor networks By Sujun Li; Siqing Yang; Suying Zhu; Fuqiang Yan; Dept. of Comput. Sci.&Technol., Hunan Inst. Of Humanities, Loudi, China in.Computer Application and System Modeling (ICCASM), 2010 International
Conference.
[9] D. Liu and P.Ning, "Establishing pair wise keys in distributed sensor networks," in Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS),Washington, DC, USA, October 27-31 2003, pp. 52–61.
[10] W. Du, J. Deng, Y.S.Han , and P.K.Varshney ,"A pair wise key predistribution scheme for wireless sensor networks," in Proceedings of the 10th ACM Conference on Computer and
Communications Security(CCS),Washington, DC,USA ,October 27-31 2003, pp. 42–51.
[11]A robust group-based key management scheme for wireless sensor networks By Zhen Yu Yong Guan Dept. of Electr. & Comput. Eng., Iowa State Univ., Ames, IA, USA Wireless Communications and Networking Conference, 2005 IEEE.
[12] Sub-Grid based Key Vector Assignment : A Key Pre Distribution Scheme For Distributed Sensor Networks(2006) By R. Kalindi , R. Kannan, S. S. Iyengar and A. Durresi of
Louisiana State University, USA.

First Author Soumyashree Sahoo continuing her MTech. Degree in Computer Science and Engineering from BPUT. She is currently a lecturer in Department of Computer Science and Engineering of Hi-tech Institute of Technology, Khurda. Her research interest includes Wireless sensor network, Cryptology and Network security.

Second Author Pradipta Kumar Mishra received his MTech. Degree in Computer Science and Engineering from IIIT-BH. He is currently an Assistant Professor in Department of Computer Science and Engineering of Hi-tech Institute of Technology, Bhubaneswar .His research interest include Ad-Hoc network, Wireless sensor network and Network security.

Third Author Prof.(Dr.) Rabi Narayan Satpathy received his PhD. Degree in Computational Mathematics and Computer Science & Engineering from Utkal University ,Odisha and cosmopolitan University and PDF From NIT,Rourkrla,Odisha & D.Sc. in computational Fluid Dynamics from FM University . He is currently the Principal in Hi-tech Institute of Technology, Bhubaneswar. His research interest include Soft Computing , Ad-Hoc network, Wireless sensor network and Network security.