Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.6, No.2, 2015
www.iiste.org

A Secure Key Management Scheme for Hierarchical WSN

Tahira Laskar Debasish Jena
International Institute of Information Technology, Bhubaneswar, India

Abstract
Many applications require WSNs to exchange sensitive information with the applications having high reliability requirements and a high level of security to succeed. The WSN nodes are often placed in hostile or adverse environment and their security concerns become a challenging issue. WSNs nodes are resource constrained and hence incorporating traditional security methods involving large computation overheads are not feasible. Key management is a fundamental part for any secure communication in WSNs. The key management system should be substantially secure, robust and efficient for a secure communication protocol. Many key establishment techniques have come up to address the tradeoffs between limited memory and security but choosing an effective scheme is debatable. Here in this paper, a new key management scheme is put forward based on authentication and key sharing for WSN. Our protocol is suitable for managing keys in a hierarchical network consisting of clusters with the aim of ensuring the survivability of the network.
Keywords: Authentication, Clusters, Key Management, Wireless Sensor Network.

1. Introduction

Wireless sensor networks (WSN) consist of a large collection of sensor nodes with each node equipped with sensors, processors and radio transceiver. Wireless sensor networks are infrastructure-less unlike traditional network like wired and Mobile Ad hoc Networks, and are capable of operating in any environment. The sensor nodes are economical and capable of performing military and civilian task such as battlefield surveillance, wildlife tracking, health-care monitoring, and natural disaster monitoring. Owing to the low cost requirement, sensor nodes should compromise on hardware complexity and have limited computation capability, storage capacity, and radio transmission range. Since sensor nodes are usually powered by batteries, limited power supply is another major concern of WSNs. WSN being often deployed in hostile environment faces the challenge of security and the exiting security mechanisms for the traditional networks are not suitable for it. Asymmetric cryptography is not suitable for most sensor networks because of increased energy consumption, large code computation and storage requirements.

Key management is the process by which cryptographic keys are generated, stored, protected, transferred, loaded, used, and destroyed[1]. Using cryptographic keys, a Key Management system establishes secure connection between nodes at network formation stage ensuring that messages are encrypted and communicating nodes are authenticated. Several alternative approaches have come up for performing key management in wireless sensor networks.

Any single key WSN system cannot achieve a very secure communication that WSN requires. This led to putting forward a hierarchical key management plan. In the hierarchical WSN key management program [4],[5],[24],[25], the nodes are divided into several clusters; each cluster has a head which controls the cluster. Key distributions of common nodes, as well as consultations and updates, are done through the cluster head. Since cluster heads are responsible to send the information within each cluster region, they themselves should be guaranteed to have high reliability.

The organization of the rest of this paper is as follows. Section 2 deals with the need for Key Management in Wireless Sensor Network. Section 3 deals Related Works while in Section the Wireless Sensor Network Model is presented. In Section 5, the Security Assumptions are made and the Notations and Symbols used in the Proposed Scheme. Section 6 deals with the Proposed Key Management Scheme while Section 7 with the Performance Analysis of the Proposed Scheme. Finally Section 8 concludes the paper.

2. Need for Key Management

Key Management in WSN is an important research area. It provides very critical security service in wireless sensor networks. But implementation of Key Management schemes in WSN is a difficult task because of the vulnerabilities of the sensor nodes and their resource limitations

Key pre-distribution phase is an important starting phase where keys are distributed before the deployment of the network, ie during the node's manufacturing time. This is followed by the key establishment phase which refers to how nodes will establish a secure session. The network formation phase is then initiated. Node addition or Node deletion phase deals with establishment of secure sessions with new nodes being added or removed from the network.

Authenticity, confidentiality, scalability, integrity and flexibility must be provided in a secure application through various key establishment techniques.

Authenticity: The communicating node should have a method of verifying the authenticity of the node with which it is communicating through the key establishment techniques.

Confidentiality: An adversary may try to access the network if it manages to obtain the secret keys to obtain the data. Confidentiality refers to the ability to protect the disclosure of data from unauthorised access. Key establishment techniques should provide confidentiality and in case of a node being compromised, it tries to keep the data from being further known.

Scalability: Key establishment techniques should provide high-security features not only for small networks but also for network of large size. Key establishment techniques if scalable can support variations in the size of the network.

Integrity: Access to the keys should be available only to the nodes within the network and only the authenticated base station should be allowed to change keys. This would stop unintended nodes from obtaining knowledge about the secret keys or from trying to change it[2].

3. Related Works

Owing to cost factor, Public key cryptosystems is not practical for WSNs and hence symmetric key primitives such as secret key encryption or cryptographic hash function are often preferred. Key management and distribution thus deals with sharing of secret keys among sensor nodes. Many Key Management schemes have been proposed for WSN. Eschenauer and Gligor [3] proposed a random key predistribution scheme based on probabilistic key sharing among the nodes of random graph. The scheme also makes it feasible for the network to be scalable since the size of the key ring and the number of keys in the ring is not fixed but can be adjusted. Chan, Perrig and Song [4] further extended this scheme through their Q-composite scheme where the communicating nodes should share at least Q number of keys. Zhu, Setia, and Jajordia introduced the localized encryption and authentication protocol (LEAP) [5] that offers different types of data switching schemes for nodes with different security requirements. Its based on symmetric key algorithms. Zhu, Setia, and Jajordia [6] further came up with LEAP+ in 2006 not targeting any specific type of sensor network but almost equally applicable to all class of static network. Every node in the sensor network maintains four types of keys according to this scheme. LEAP+ is not suitable for dynamic network since the energy consumption overhead in establishing communicating links is high. Blundo et al.[6] proposed several schemes which allow any group of t parties to compute a common key, while being secure against collusion between some of them. Blundo et al. [7] distributes a polynomial share to each sensor node by using which every pair of nodes can generate a link key. Panja *et al.* [8] describe group key management protocol for hierarchical sensor networks consisting of different groups, each with unique key. The sensor nodes in a group don't use pre-deployed keys but dynamically generate partial keys using a function that takes partial keys of its children as input. The group key management protocol by Panja *et al.* [8] offers high scalability and flexibility with less storage and computation cost. For hierarchical clusters, Hu etal. [9] gave a Secure Power-Efficient Clustered-Topology Routing Algorithm (SPECTRA), that combines routing and key management to provide an energy efficient security and routing solution.

4. Wireless Sensor Network Model:

The network consists of all the nodes organised in clusters. Each cluster consists of a cluster head and a number of sensor nodes as shown in the figure below.

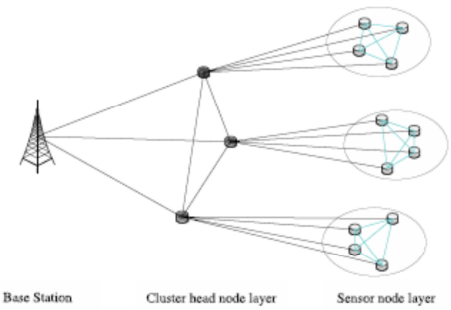

Fig. 1. Hierarchical wireless sensor network model.

Communication takes place between the sensor nodes and the cluster head as well as between the cluster heads and the Base Station (BS) of the network. A base station is typically a gateway to another network, a powerful

data processing/storage centre, or an access point for human interface [13]. The sensor nodes in the cluster send the data to the cluster heads. The Cluster heads aggregates the data received from its member nodes and sends it to the Base Station. The communication between the Base Station and the cluster heads may also be multihop with the Base Station located far away from the cluster heads.

5. Security Assumptions

The following assumptions are made as in most of the sensor nodes for security schemes [3], [4], [10], [11], [12]:

- The Sensor nodes are synchronised with each other in time.
- The sensor nodes have a unique ID (identifier) of length long enough to differentiate one from the other.
- The Base Station has a member table of node IDs and their corresponding secret sensor keys. The table is updated every time a node enters or leaves the network.
- The Base Station has immense computational power and memory storage capacity and is located in a well protected place.
- The Base Station has an authentication system [11] that works for any node in the network.
- It is assumed that an adversary needs at least T_{cap} time to capture a node and then collect the information from the node [12].

Notations

The following notations are used to describe the security protocol:

Notation	Description
BS:	Base Station
CH_j:	Cluster Head of jth cluster.
ID_i:	Identity of node S_i
$E_k(Msg)$:	Encryption of message, Msg with key k.
$MAC_k(Msg)$:	Message authentication code for message Msg, generated using key k.
nounce:	A random String number.
adv:	Advertisement message generated by CH.
$data_1$:	Data from node 1.
$F(data_1, data_2, ..., data_n)$:	Data aggregation function.
Network Key (K_N):	A globally key that is shared by all nodes in the network and the BS.
Sensor Key (K_{si}):	Generated by the base station, based on a seed and sensor ID, pre-deployed in each sensor node and shared by the sensor nodes and base station.
Initial Key ($K_{i.}$):	Pairwise shared key between the sensor node, Si and the base station. It's used only once to authenticate the nodes from the Base Station.
T_{epoch}:	An epoch which refers to the time period which is less than the time required to capture a node.
| | :	Concatenation Operator

6. Proposed Key Management Scheme

In our approach the nodes use a pre-deployed symmetric keying technique. Some of the features specified in [15],[22] are also being taken into consideration and further extended. Sensor nodes should be assigned minimum number of keys as they are memory constrained and are susceptible to attacks by the adversary. In case of a node being captured, it also helps to reduce the impact of the damage since less number of keys would be revealed to the adversary.

Here, a new key management scheme put forward based on authentication and secret key sharing for WSN. Our protocol is suitable for managing keys in a hierarchical network consisting of clusters with the aim of ensuring the survivability of the network. Each node is pre-deployed with a sensor key which is known to the Base Station, BS. Initially the sensor network is formed with each node in the network in possession of the common network key dynamically generated by the BS. The clusters are next formed with the Cluster Head, CH being informed of the sensor key of each of the sensor node in the cluster. Data communication takes place within the cluster with the messages being encrypted by the sensor key of the node communicating with the CH. Data transfer between the cluster head, CH and the BS are encrypted by sensor key of the CH. The sensor keys and the network key are periodically refreshed to avoid an adversary from attacking the network. Since the CH is responsible for processing of the data in cluster and transmission to BS, it has relatively large energy consumption and is to be replaced periodically to balance the energy cost. Our protocol provides seven efficient security administration mechanisms:

1) Node Deployment 2) Network Initiation 3) Cluster Initiation 4) Data Transmission 5)Key Refreshing 6) Node Addition 7)Re-clustering. All of these mechanisms aim to localize the impact of attacks and considerably improve the efficiency of maintaining fresh sensor keys and the network key.
Our Scheme consists of the following phases:

6.1 Node Deployment Phase:

In this phase, Nodes transmit Hello message to its neighbors along with its ID. The nodes that are within the radio range of the requesting node reply with their IDs. The requesting node creates database consisting of table of neighbors.

6.2 Network Initialization Phase:

In this phase, the sensor nodes and Cluster Heads are authenticated by the Base Station. The Initial key *Ki* that's being pre-deployed in the sensor node, S_i is used to authenticate the node. The key is then erased from node memory after being used for authenticating the node.
The steps followed in this phase can be stated as follows:

Step1: Node S_i send authentication packet to the base Station by inserting its ID, generating a nounce, encrypting the message and calculating MAC value on it using its Initial key $K_{i.}$
S_i => BS: [IDi , nounce, E_{ki} (IDi ,nounce) , MAC_{ki} (IDi ,nounce)]
BS authenticates the node by verifying the encryption and the MAC using that node's Initial key.

Step 2: BS generates the new network key $K_{N,}$ encrypts with Initial Key, $K_{i.}$ and broadcasts it to all other nodes in network. Here it is transmitting it to the Sensor node $S_{i.}$
BS => S_i: [E_{ki} (K_N)]

Step 3: Node S_i decrypts the encrypted value of the network key K_N using the Initial key $K_{i.}$. It then deletes Initial key $K_{i.}$ from its memory. Thus the network is formed with all the sensor nodes in the network sharing the globally common network key $K_{N.}$

6.3 Cluster Initialization Phase:

In this phase, the clusters in the network are formed and authenticated by the BS.

Step 1: The Cluster Head, $CH_{j,}$ which may either be selected or elected authenticates itself to the BS by sending a packet consisting of its ID & nounce. The CH ID & nounce is also encrypted with the sensor key of $CH_{j,}$ K_{CHj} and the MAC value calculated on it by the CH's sensor key, $K_{CHj.}$

CH_j => BS: [$ID_{CHj.}$, nounce, adv, $E_{KCHj.}$(ID_{CHj},nounce,) , MAC_{KCHj}(ID_{CHj},nounce)]

Step 2: BS authenticates the CH by verifying the encrypted value and MAC using the sensor key of CH, $K_{CHj.}$

Step 3: BS broadcast the Cluster Head ID and it *adv* by encrypting it with network key.
BS => *: [ID_{CHj} , E_{KN} (adv)]

Step 4: The nodes receiving the *adv* take note of the signal strength of the received advertisement and the corresponding Cluster Head IDs. The nodes send membership message to the CH whose signal strength is strongest.
For membership to cluster Head $CH_{j,}$ Sensor Node S_i generates message M consisting of its own identifier $Id_{i,,}$ the identifier of the intended cluster Head ID_{CHj} and it own sensor key, $K_{si.}$
M= (Id_i || ID_{CHj} || K_{Si})
Node S_i then encrypts the message M with the network key, K_N along with the MAC value calculated on it using the network key, K_N. Node S_i also sends a join request, *join-req* along with its identifier and that of its cluster head.
S_i => CH: [$ID_{i.,}$ $ID_{CHj,}$ nounce, join-req, E_{KN} (M) , MAC_{KN}(M)]
At the end of this phase, the CH collects all the secret sensor keys of its group members. The CH builds a member table consisting member node IDs and their sensor keys.

Step 5: Cluster Authentication Phase: The CH calculates the authentication code for itself and its members using one way hash function [14] as:
H1 = H (Ks1, K_{CHj})
H2 = H (Ks2, H1)
……..
Hn = H (Ksn, Hn-1) , where K_{CHj} is sensor key of CH and Ks1, Ks2.…Ksn are the sensor keys of member nodes S1, S2 , … Sn .
CH encrypts its IDs and hash values with its secret key, K_{CHj} and sends it to BS.
CHj => BS: [ID_{CHj}, $E_{KCHj.}$ ($ID_{CHj.}$, $ID_{1,}$, $ID_{2,....}$ ID_n...H1, H2,.... Hn)]

BS authenticates the group by computing these values again.[15]

6.4 Data Transmission Phase:

Step 1: Member nodes encrypt the data packets using its own sensor key, which is again encrypted by the network key K_N. Each node S_i then sends it to its Cluster Head CHj.

S_i => CHj: [$ID_{i.}$, $ID_{CHj,}$ $E_{KN.}(E_{KSi}(data_{Si}))$]

Step 2: *CH* decrypts all the encrypted data sent from member sensor nodes, aggregates and then encrypts them by the sensor key and then by network key and sends the data to BS.

CHj => BS: [$ID_{CHj,}$ E_{KN} (E_{KCHi}(F($data_1$, $data_{2,}$ $data_{3.....,}$ $data_n$)]

6.5 *Refreshing of keys:*

A single key encrypts significant amount of data. If an adversary has information about the sent data and its format, it is likely that he can conduct a known plaintext attack. A remedy to this threat is to renew the encryption keys periodically [17].

The network key and sensor keys are periodically authenticated. After every time period T_{epoch} , the BS regenerates the network key and sensor keys as explained below:

Step 1: For Network Key E_{KN} , BS periodically broadcasts a new network key, $NewK_N$ by encrypting it with current network key. Sensor nodes decrypt it with the current network key and get the refreshed network key.

BS => *: [E_{KN} ($NewK_N$)]

Step 2: For sensor key K_{si} of each sensor node S_i , BS also broadcasts a new Sensor key, $NewK_{Si}$ encrypting it with current sensor key. Sensor node S_i decrypts it with the current sensor key and gets the refreshed sensor key.

BS => S_i: [E_{KSi} ($NewK_{Si}$)]

6.6 Node Addition Phase:

New nodes that enter the network are first authenticated and then get the current network key. Based on its distance from the BS, the BS also broadcasts the ID of the Cluster Head closest to the new node. The new node then sends to the CH, a *join request* consisting of its ID, nounce, MAC and encryption performed on this two values using current network key. The method proceeds from step 4 of 6.2 section.

6.7 Re-clustering of the WSN phase:

After a certain time interval, a new cluster is formed to balance the energy consumption of the current cluster head [16]. After cluster duration T_{ch} , BS broadcast a message to the current cluster heads to erase its member ID table. New Cluster formation process starts as discussed in section 6.3 and the process continues.

7. Performance Analysis

7.1 Security Analysis

Data Confidentiality is achieved by use of symmetric encryption techniques. Use of multiple encryption keys makes compromise exponentially difficult. Data integrity and entity authentication are accomplished by sending the message together with MAC in every message transmission. It is required for the communicating entities to perform MAC verification with the received message before accepting it.

Each Sensor node has a unique key shared with its CH. So compromise of any sensor node won't affect the secure communication between the CH and its other members. Moreover if a CH is captured or its energy exhausted, the key stored on it will not be of any use since the keys will be refreshed. This periodic refreshing of key information is triggered by the BS. So even if the attacker captures CHs of different time quantum, it can't reconstruct the network key. Thus, our scheme provides sufficient security and can achieve a reasonable degree of resilience.

7.2 Communication Overhead

The communication overhead of our scheme is incurred during the network key establishment, pair-wise keying between member node and CH and finally during key refreshment method. It also requires an authentication process to establish the network key and pair-wise keys in each cluster. A total of two transmissions are required to establish the network key and two transmissions are required to establish the pair-wise key between member node and CH. The effect of increasing cluster size is considerably insignificant.

7.3 Storage Complexity

IEEE 802.15.4 Low-Rate Wireless Personal Area Network (WPAN) standard have defined device ID as 64-bit

[20]. We consider the node ID length to be of 64-bit, generated nonce value of 16-bit, and MAC output as 32-bit as proposed by Zoltak et. al [18] and Karlof et al. [19]. Here we assume that symmetric encryption scheme requires 128-bit keys. In this case, the longest message would take up around 38 bytes. This message length can accommodate into one sensor nodes packet payload per communication.

For a given a sensor network of size *n*, a public key scheme would require a large storage space for keys and certificates. A random key scheme would require to store *n* number of keys and a pairwise symmetric scheme would require to store 2*n* number of keys. As compared to most of the other key management schemes, the storage overhead of our protocol is substantially small and independent of the network size. Our scheme requires only an initial key which is then replaced by the network key and the sensor key to be stored in each sensor node. [21]

Analysis of Key Management Schemes:

Key Management Schemes	Keys per sensor node	Scalability	Nodes affected in case of Intrusion
Public Key Cryptographic scheme	2	Node-to-Node Authentication	All sensors communicating with the compromised node
random key scheme	N	Simple with probability p	All sensors sharing the same set of n keys with the compromised node
Pairwise symmetric scheme	2n	Node-to-Node Authentication	All sensors communicating with the compromised node
Merkle Tree	1 + log n	Complex tree operation	All sensors communicating with the compromised node
Our Scheme	2	Node-to-Node Authentication	All sensors communicating with the compromised node

8. Conclusion

Many researchers have worked on Key management for Wireless Sensor Networks (WSNs) which is a very critical issue from the security point of view. In this paper, a key Management Scheme based on clustering in WSN has been presented. It provides security and resilience with reasonably less communication overheads. In our further research, we will further probe into the possible attacks in our scheme and simulate it. We also plan to implement it in the real scenario and prove the feasibility.

References

[1]J. C .Lee, Victor C., M. Leung, Kirk H. Wong, Jiannog Cao, and Henry C. B. han(2007): "Key Management Issues In Wireless Sensor Networks: Current Proposals And Future Developments", Proceedings of IEEE Wireless Communications, p.p. 76-84.

[2],Yang Xiao, Venkata Krishna Rayi, Bo Sun, Xiaojiang Du, Fei Hu, and Michael Galloway "A Survey of Key Management Schemes in Wireless Sensor Networks"

[3] L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," *Proc. 9th ACM Conf. Comp. and Commun. Sec.*, 2002, pp. 41–47.

[4] Chan, H., Perrig, A., and Song, D. 2003. Random Key Predistribution Schemes for Sensor Networks. In Proceedings of the 2003 IEEE Symposium on Security and Privacy (May 11 - 14, 2003). SP. IEEE Computer Society, Washington, DC, 197-213.

[5] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," *Proc. 10th ACM Conf. Comp. and Commun. Sec.*, 2003, pp. 62–72.

[6] Zhu, S., Setia, S., and Jajodia, S. 2006. LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Trans. Sen. Netw.*

[7] Blundo, C., Santis, A., Herzberg, A., Kutten, S., Vaccaro, U., and Yung, M. 1992. Perfectly-secure key distribution for dynamic conferences. In Crypto 92.

[8] B. Panja, S. K. Madria, and B. Bhargava, "Energy and Communication Efficient Group Key Management Protocol for Hierarchical Sensor Networks," *SUTC '06: Proc. IEEE Int'l. Conf. Sensor Networks, Ubiquitous, and Trustworthy Comp.*, 2006, pp. 384–93.

[9] Hu, F., Siddiqui,W., Cao, X.: Spectra: Secure power-efficient clustered-topology routing algorithm in large-scale wireless micro-sensor networks. International Journal of Information Technology 11 (2005)

[10] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 1, p. 597, 2004.

[11] Donggang Liu, Peng Ning, "Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks" in: Proceedings of the 10th Annual Network and Distributed System Security

Symposium, San Diego, California, February 2003, pp. 263–276.
[12] Fei Hu, Waqaas Siddiqui, Krishna Sankar, "Scalable security in Wireless Sensor and Actuator Networks (WSANs): Integration re-keying with routing", Computer Networks 51 (2007) 285–308, Science Direct, Elsevier.
[13] Shen & Shi:" A Dynamic Cluster-based Key Management Protocol in Wireless Sensor Networks", INTERNATIONAL JOURNAL OF INTELLIGENT CONTROL AND SYSTEMS, VOL. 13, NO. 2, JUNE 2008, 146-151
[14] Bart Preneel, "The State of Cryptographic Hash Functions", Lectures on Data Security, pp. 158-182, Springer, 1999.
[15] Md. Ibrahim Abdullah, " A Key Distribution and Management Scheme for Hierarchical Wireless Sensor Network" International Journal of Multimedia and Ubiquitous Engineering Vol. 6, No. 3, July, 2011
[16] W.R. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy efficient communication protocol for wireless microsensor networks", in: Proceedings of the 33rd Annual Hawaii International Conference on System Sciences (HICSS), January 2000, pp. 3005–3014.
[17] W. Fumy and P. Landrock, .Principles of key management,. IEEE Journal of Selected Areas in Communications, vol. 11, pp. 785-793, June 1993.
[18] Zoltak, B., "Tail-MAC: An Efficient Message Authentication Scheme for Stream Ciphers", Cryptology ePrint Archive, Report 048 (2004)
[19] Karlof, C., Sastry, N., Wagner, D., "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems (SenSys 2004), pp.162-175 (2004)
[20] Naveen Sastry, David Wagner, "Security Considerations for IEEE 802.15.4 Networks", ACM Workshop onWireless Security WiSe 2004, October 2004.
[21] Shu Yun Lim , Meng-Hui Lim,"Energy-Efficient and Scalable Group Key Management for Hierarchical Sensor Network", Journal of Ubiquitous Systems & Pervasive Networks
[22] Firdous Kausar, Ashraf Masood, and Sajid Hussain, "An Authenticated Key Management Scheme for Hierarchical Wireless Sensor Networks" in: Recent Advances in Communication Systems and Electrical Engineering (CSEE), Lecture Notes in Electrical Engineering , Springer, Volume 4, pp 85-98, 2008.
[23] Perrig A, Szewczyk R, Tygar J, Wen V, Culler D. SPINS: Security protocols for sensor networks. ACM Wireless Network, 2002,8(5):521−534.
[24] Younis M, Ghumman K, Eltoweissy M. Location-Aware combinatorial key management scheme for clustered sensor networks.IEEE Trans. on Parallel and Distribution System, 2006,17(8):865−882.
[25] Eltoweissy M, Moharrum M, Mukkamala R. Dynamic key management in sensor networks. IEEE Communications Magazine,2006,44(4):122−130.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar