Key Distribution Schemes in Wireless Sensor Networks: Novel Classification and Analysis

Premraj Mahajan and Anjali Sardana

Electronics and Computer Science Department,
IIT Roorkee, India
{prem228434,dr.anjalisardana}@gmail.com

Abstract. Security is one of the important and challenging aspects in wireless sensor network owing to their wireless nature combined with limited memory, energy, and computation. We can classify security issue of the wireless sensor network into five broad categories as cryptography techniques, key management, routing protocols, intrusion detection and data aggregation. Since the key management forms an underlying factor for efficient routing protocol and cryptography in wireless sensor network, we focus on key management issue. This paper outlines the constraints, security requirements and attacks, which are related to the key management and routing. Further novel classification of key distribution schemes have been proposed. The proposed novel classification and comparison distinctly brings to the fore gaps in the existing solutions of research which can be put to use by researchers in the area to identify current challenges for designing efficient key distribution scheme. The paper concludes with possible future research directions on key distribution in WSNs.

Keywords: Key distribution schemes, Security, Sensor network.

1 Introduction

Wireless Sensor Network contains hundreds or thousands of sensor nodes and these sensor nodes have the ability to communicate either amongst each other or directly to an external base station (BS). Figure 1 shows a schematic diagram of sensor node components. Basically, sensor node comprises of sensing, processing, transmission, mobilizer, position finding system, and power units. The same figure shows the communication architecture of a wireless sensor network (WSN) [1, 2].

These types of the sensor nodes are deployed into the field for the purpose of sensing some specific information. But these sensor nodes are resource constraints. Sensor nodes have limitations like computational power, storage, battery etc. So possibility of the attacks like hello flood on sensor node is more. Hence it is important to utilize available resources effectively with fulfilling the basic requirements like encryption, authentication etc. These (encryption, authentication) services are based on operations which involves the different [3]keys like encryption-decryption keys, cluster key, key which is used in hash function etc. So energy efficient key distribution in sensor nodes plays vital role in security of WSNs Section 2 of this paper presents constraints of the wireless sensor network along with security requirements. Section 3

N. Meghanathan et al. (Eds.): Advances in Computing & Inform. Technology, AISC 176, pp. 43–53.
springerlink.com

presents attacks related to the key management and routing. In section 4, a novel classification of the key management schemes is presented. Section 5 discusses about conclusions and future work to be done.

2 Constraints in Wireless Sensor Network

Sensor nodes have limited processing power, storage capacity and transmission range because of the energy and the physical size.

Energy: Energy in sensor network is conserved for many purposes like sensing, ADC, computation, communication. So for long lasting working of the sensor, all these operations should be performed efficiently.

Computation: Embedded processors in sensor nodes are not so powerful that they can perform the complex cryptographic functions. Typically 8bit, 4-12 MHz[4].

Memory: Memory includes flash memory and RAM. Flash memory is used for storing downloaded application code and RAM is used for sensed data, intermediate computation. In SmartDust project, tiny OS code space is 3500bytes, and only 4500bytes [4] are there for the security application.

Transmission range: Again range is also dependent on the energy limitation. It also depends on the environment factors like whether and terrain.

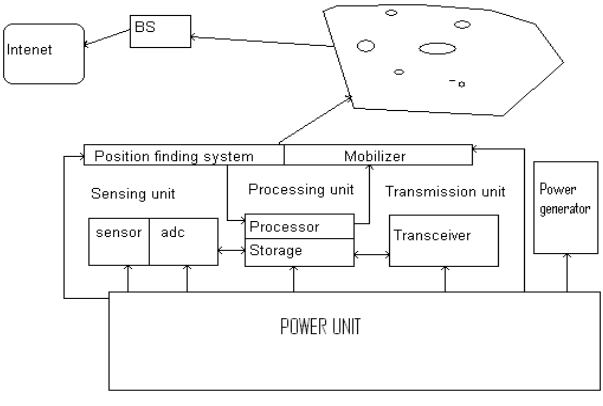

Fig. 1. The component of sensor network [3]

Security requirement: To protect the information and resource from attacks, security services are provided in WSNs. These security requirements include:

- **Authentication:** It ensures that communicating nodes are genuine and no any malicious node can inject or spoof the message.
- **Availability:** It ensures that message is made available to the destination node even in presence of the intermediate node capture or Denial-of-service attack.

- **Authorization:** It ensures that only authorized nodes can be involved in providing information to network services.
- **Confidentiality:** It ensures that the given information cannot be understood by the attacker or any unauthorized person.
- **Integrity:** It ensures that information cannot be altered by any intermediate malicious node.

3 Attacks Related to Key Management and Routing

Wireless Sensor Network is vulnerable to various types of attacks. In following section the attacks which are related to key management and routing are considered.

Spoofing, altering and replaying attack: In presence of the spoof and replay attack, the network traffic can be extensively corrupted. Continuous alteration in the message transmits the incorrect message and source node has to retransmit the packets. It reduces the battery life in large extend due to power exhaustion. In replay attack, malicious node may capture the any of the network message and replay that message, and hence damaging the network performance.[4, 5]

Selective forwarding attack: Normally sensor nodes are multi-hop systems and the assumption in such network is that intermediate nodes faithfully forward the received message. In this type of attack the malicious node may refuse or simply drop some part of message [4-6]. Such type of attack is most effective when attacker is explicitly included on the path of data flow.

Sybil attack: The Sybil attack is a case in which malicious node shows multiple identities. Malicious node behaves as it is a large number of the nodes for example impersonating other node or simply claiming false identities. In worst case, an attacker may generate an arbitrary number of additional node identities, using single device [4, 7].

Sinkhole attack: The attacker tries to pass nearly all the traffic from a particular area through a particular/malicious node. An attacker makes a compromised node look more attractive to the surrounding nodes by forging routing information and ultimately surrounding nodes will choose next node to route the information through the compromised node giving access to all data. Many attacks can be initiated [4, 5] through the sinkhole attack ex. Wormhole, selective forwarding or eavesdropping.

Wormhole attack: A wormhole is low-latency link between two portions of the network over which attacker replays the network messages [5, 8]. An attacker receives the packets at one portion of network and tunnels them to another portion, and then replays them into the network. These tunneled packets arrive sooner than the other packets transmitted over normal multi-hope route because these tunneled distances are longer than the normal wireless transmission range of a single hop. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality.

Hello flood attack: Many of protocol use HELLO packets for getting the list of the neighboring nodes and assume that replied nodes are within their transmission range and are therefore neighbors. But an attacker may use high-powered transmitter to

track maximum areas[5] so that, other nodes will believe that they are neighbor. If the attacker falsely broadcast a superior route to the base station then all nodes will pass the information through those attacking nodes even that node is out of range.

Acknowledgement spoofing attack: Acknowledgements are sometimes required in the sensor networks. An attacker node can spoof acknowledgements. Goal of the spoofing the acknowledgement is that attacker can convince[5] the sender node by giving false information like a weak link as strong or dead node as alive.

Tampering attack: Tampering is a physical layer attack. Given physical access to node, attacker can extract sensitive information such as cryptographic keys and some other data on a node [9] and may create false identity.

Table 1. Different types of attacks and their defense mechanism along with related issue

TYPES OF ATTACK	DEFENSE MECHANISM	ISSUE
Tampering	a. Tamper-proofing b. Hiding	High cost
Spoofed, Altered, or Replayed Routing Information	a. MAC b. Monitoring c. Lightweight Authentication d. SPINS protocol	Computation power Computation power
Selective Forwarding	a. Multi path routing b. Probing	Computation power
Sinkhole	a. Authentication b. Geographical routing c. Redundancy d. Monitoring	Computation power, key distribution Energy consumption
Sybil	a. Use of symmetric keys b. Probing	Computation power, key distribution Energy Consuming
Wormhole	a. Authentication b. Time synchronization c. Packet leashing by geographical and temporal information	Computation power, key distribution Infeasible
Hello flood Attack	a. Authentication b. Verify the bidirectional link	Computation power, key distribution
Ack. Spoofing	a. Authentication	Computation power, key distribution
Node replication attack	a. Localized voting system b. Key renewing	Replication attacks

4 Key Distribution Schemes

In wireless sensor network, to provide the basic security requirement like encryption, decryption, authentication etc. we have to perform some operations involving the different types of keys. With considering the constraints of the sensor node, we have to distribute these keys to all the sensor nodes. This key distribution operation must be energy efficient so as to increase the life-time of sensor node. An open research problem is how to set-up secrete keys among the communicating nodes. There are different schemes are proposed for key distribution among the sensor nodes. These schemes are categorized with the following properties [3, 10, 11]:

- **Pre-distribution/Post-distribution:** In pre-distribution schemes the keys are stored into nodes before deployment into the field and in post-distribution schemes the keys are distributed after the deployment into the field with the help of trusted server or self-enforcing property.
- **Homogeneous/Heterogeneous:** In homogeneous sensor network, all the nodes are identical and having the same computational power, storage capacity and energy level whereas in case of the heterogeneous sensor network, small number of sensor nodes are more powerful in terms of the energy, storage and computational power than other large number of the sensor nodes.
- **With deployment knowledge/without deployment knowledge:** Sensor network which knows that where and how the sensor nodes are deployed into the network that comes under deployment knowledge category. And other sensor networks, which don't have information about the deployment knowledge, that comes under without deployment knowledge category.

Different types of key distribution schemes are classified as shown in the figure 2:

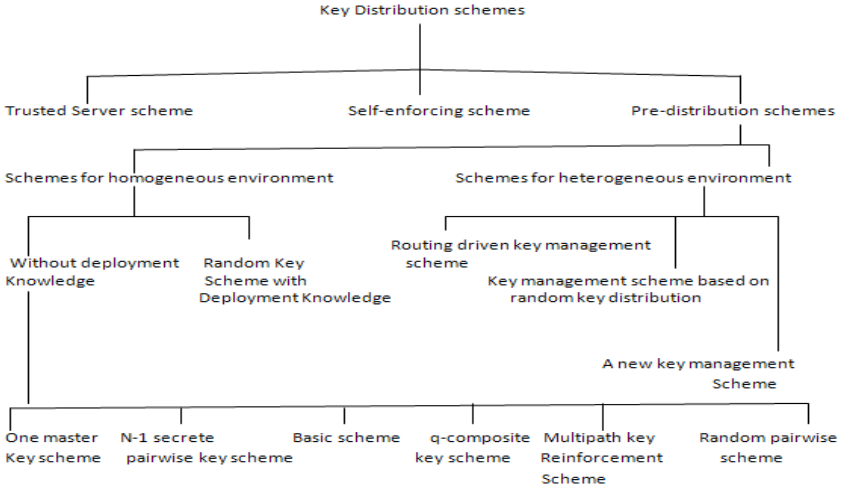

Fig. 2. Classification of key distribution schemes

4.1 Trusted Server Scheme

Trusted server scheme depends on the trusted server for key agreement between two different nodes, e.g. Kerberos. Such a third party key distribution requires infrastructure which is impractical [11, 12]for sensor network.

4.2 Self-enforcing Scheme

Self-enforcing scheme depends on asymmetric cryptography. it is very good solution for key management and distribution in WSN but sensor nodes have lot of limitations

like memory and processing power. Limited computation and energy resources of the sensor nodes often make it undesirable to use public key algorithms, such as Diffie-Hellman key agreement or RSA. Several works shows[13] that lightweight versions of the public key algorithms can be utilized in the sensor networks.

4.3 Pre-distribution Schemes

In pre-distribution schemes the keys are stored into nodes before deployment into the field. These can be further divided into schemes for homogeneous and heterogeneous environment.

4.3.1 Schemes for Homogeneous Network

In homogeneous sensor network, all the nodes are identical and having the same computational power, storage capacity and energy level.

4.3.1.1 Without Deployment Knowledge. In these schemes, deployment knowledge is not considered.

4.3.1.1.1 One Master Secrete Key Scheme [11]: In one master secrete key scheme, each node carry one master key, pre-distributed before deployment. This master key is used to achieve the key agreement and obtain a new pair wise key. Because of one master key, this scheme doesn't exhibit desirable network resilience. If any node is compromised then the entire sensor network will be compromised. In this scheme giving the temper proofing mechanism, will increase the cost as well as energy consumption of each node.

4.3.1.1.2 N-1 Secrete Pair-Wise Key[11]: In N-1 secrete pair-wise key scheme, if there are N nodes then each node should have to carry n-1 secrete pair-wise keys. Each of which is known to this sensor and one of the other to n-1 sensor node. Resilience is perfect as compared to other scheme because if any of the nodes is compromised then that node does not affect the security of communications of other nodes. But this system has main two drawbacks. It is not practical because of extremely limited amount of memory. As the network grows (N), memory required for storing keys also increases. Second one is, adding new node to pre-existing network is complex because the existing nodes do not have the keys of the new sensor node.

4.3.1.1.3 Basic Scheme [14]: It consists of three phases. Key pre-distribution, shared key discovery and path key establishment. First phase store small number of the keys into nodes key ring, taken from generated pool of keys to ensure that two node share at least one key with a chosen probability. Second phase establishes the secure link between two nodes only when they carry secrete key common. Third phase assigns the path-key to selected pairs of sensor nodes in wireless communication range that do not share a key but are connected by two or more two or more links at the end of the shared key discovery phase.

4.3.1.1.4 q–composite Key Scheme [10]: In previous scheme, we require common single key from key rings of two communicating nodes in order to secure link in the key–setup phase. In q –composite key scheme, q>1 common keys are needed. In this

way it increases the resilience of the network against node capture. This scheme uses Merkle puzzle in key set-up phase. After key set-up and discovery a new communication link key is generated as: $K = \text{hash}(K_1||K_2||\ldots||K_q)$ and hashed in canonical order. This scheme has no resistance against node replication since node degree is not constrained and there is no limit on the number of times each key can be used.

4.3.1.1.5 Multipath Key Reinforcement [10]: This method conjunction with basic scheme strengthens the security of an established link key by establishing the link through multiple paths and improves the resilience against node capture. Key set-up is as per basic scheme. Then each link is secured using a single key from key pool. This single key may be the part of any other node and if that node is captured then the link may not be secured further. So to address this problem, multipath reinforcement scheme update the communication key to a random value after key set-up through multiple paths between the nodes. The more the path we can find between the nodes, the more security multipath key reinforcement provides for the link between any two nodes. A link is considered completely compromised if all its reinforcement paths are also compromised.

4.3.1.1.6 Random Pairwise Key scheme [10]: In initialization phase, a node can only store random set of np pairwise keys where n is total nodes can be used in sensor network and p is probability. Total n node unique identifiers are generated. Size of network may be less than n and other unused identifiers are used for future network expansion that means provides some range of scalability. In post-deployment key set-up phase, each node first broadcasts its node ID to its immediate neighbors. Scheme provides node-to-node authentication by using identifiers. Provides distributed node revocation with adding some overhead in key storage and provides perfect resilience against node capture as it does not reveals any information about links.

4.3.1.2 With Deployment Knowledge. In pre-distribution schemes the keys are stored into nodes before deployment into the field

4.3.1.2.1 ABAB Scheme [15]: This scheme uses approximate deployment prior knowledge to improve the performance of a random key pre-distribution scheme. Motivation of this scheme is to design simple, flexible key distribution scheme[14] that are easily applicable, extensible and sufficiently secure. This scheme uses two large key pools for overall network with some common keys in common. This scheme is totally based on “the basic scheme”.

4.3.1.2.2 ABCD Scheme [15]: ABAB scheme is easily applicable in sensor network but it has a resilience problem since same keys are used in different zones several times. ABCD scheme is more complex than ABAB but it is more efficient and resilient scheme as it uses 2r keys pools, where r is the number of rows of deployment. Direct key and path key establishment is as per the basic scheme.

4.3.2 Schemes for Heterogeneous Network

In homogeneous scheme, it is assumed that all sensor nodes are of same power and same capacity. But the works have suggested [16]that connectivity, lifetime, reliability and resilience can be improved substantially if few nodes are given greater power and transmission capacity.

Some Common Assumptions of heterogeneous sensor network environment are:

- There are two types of sensor nodes H (powerful and provided with temper-resistance) and L (ordinary).
- Each L nodes and H nodes have unique node ID.
- Routing in Heterogeneous sensor network consists of two phases:
  1. Intra cluster routing (each L sensor sends data to its cluster Head)
  2. Inter cluster routing (Each cluster head sends may aggregate data from multiple

L-sensors and then sends compressed data to sink via the H-sensor backbone.

Following are some heterogeneous key distribution schemes in heterogeneous wireless sensor network:

4.3.2.1 Routing Driven Key Management Scheme [17]: This scheme is referred as ECC based key management scheme. This scheme requires only small number of ECC computations in each L-sensor as compared to ECC public key cryptography. Server generates pair of ECC public and private keys, one pair for each L-sensor and H-sensor. Each H-sensor are pre-loaded with public keys of all the L-sensors, association between each L-sensor and its private key, and a special key K_h, which is used by a symmetric cryptography algorithm for verifying newly deployed sensors and for secure communications. Each L-sensor is pre-loaded with private key and public keys of H-sensors. In this scheme it is assumed that each L-sensor can determine its location. L-sensor sends key request message to H-sensor, which include its location and its ID via shortest distance path. After receiving the request message, H-sensor uses MST or SPT algorithm to determine the tree structure in the cluster. Then H-sensor generates shared keys for each L-sensor and its c-neighbors, Then H-sensor unicasts the message to respective L-sensor node with their private key. After receiving the message L-sensor decrypt the message and communicate securely with their neighbors. The scheme utilizes the fact that a sensor node communicates with a small portion of neighbors only and thus greatly reduces the communication and computation overheads of key set-up as compared to homogeneous schemes. It Stores small number of keys into the L-sensor.

4.3.2.2 Key Management Scheme Based on Random Key Distribution [3]: This scheme pre-load only one secrete key of key pool into L-sensor generate new key by applying one way function on key and its ID. H-sensors are pre-loaded with all keys of key pool along with a special master key for inter cluster communication. With Hello message L-sensor and H-sensor find their neighbors and then L-sensor sends the list of its neighbor to the H-sensor. After that H-sensor generates the data encryption key and integrity check key and forwards the MAC check along with nonce. After receiving the nonce L-sensor calculates the data encryption key and integrity check key. After setting the keys, Ha generates the shared pair-wise keys between a node and its neighbors. This scheme significantly reduces the storage requirement as compared to random key pre-distribution schemes.

4.3.2.3 A New Key Management Scheme [18]: During cluster formation this scheme scheme obtains the distance between the cluster head and other sensor nodes. This

scheme uses the concepts of level, as each level has separate seed used for deriving the new keys that are only used in that level and neighboring level. The key pool consists of base key and derived keys. Derived key are hash of base keys with different seeds. In pre-distribution phase, scheme stores only base key and not derived key. It stores randomly k keys into each sensor and c base keys into each H-sensor where c>>k. Pair-wise key between sensor and base station is stored in L-sensor and will be used for authentication purpose. Each CH sends location to base station by GPS and obtains the maximum distance a point can have in his cluster. In this scheme, the number of base keys has effect on connectivity between nodes and number of seeds has effect on resiliency against node capture.

Table 2. Comparison of key distribution schemes

Scheme	Pre-distribution	Deployment knowledge	Hetero-geneity	Features	Drawback
Trusted serevr [11]	No	No	No	1.Good Resilience to attack 2.Low memory required.	1.Require third party 2.Trust issue
Self enforcing [13]	No	No	No	1.Easy node addition. 2.Good Resilience to attack. 3.Most secure	1.High computational power 2.Large memory
One master key [11]	Yes	No	No	1.Easy node addition 2.Low Memory required	1.Bad Resilience to attack
N-1 pair-wise secrete key [11]	Yes	No	No	1.Better Resiliecne to attack	1. Node addition Difficult 2.Large memory required
Basic scheme [14]	Yes	No	No	1.Good Resilience to attack. 2.Easy Node addition.. 3.Simple method	1.Large Memory required
q-composite scheme [10]	Yes	No	No	1.More resilience to attack 2.Support Large network	1.Large memory required
Miltipath Key reinforcement [10]	Yes	No	No	1. Strongly secure links 2.Good resilience agianst node capture.	1.Add overhead key estabilishment traffic. 3.Large Memory required.
Random pair-wise scheme [10]	Yes	No	No	1.Provides node-to-node authentication. 2.Good resilince aginst node attack.	1.Large Memory required. 2.Scalable to some extend.
ABAB [15]	Yes	Yes	No	1.Very simple and flexible. 2.Less secure 3.Very much scalable.	1.Required prior deployment knowledge 2.Large Memory required
ABCD [15]	Yes	Yes	No	1.More secure than ABAB. 2.Highly scalable. 3.Requires less communicational cost.	1.Complicated than ABAB. 2.Required Prior deployment knowledge.
Routing driven [17]	Yes	No	Yes	1.Highly secure and scalable 2.Low memory storage.	1.Sensor node has to send its location through GPS.
Key mgnt. scheme based on random key distribution [3]	Yes	No	Yes	1.Better resillience to attack. 2.Low memory required. 3.Low computational cost. 4.Addition of node is easy.	1.Scalable to some extend. 2.H sensor exhuastion may occur with large network
A new key management scheme [18]	Yes	No	Yes	1.Reduces tradeoff between resilience and connectivity. 2.Require low memory.	1.Sensor node has to send its location through GPS.

Table 2 gives the comparison of the different key distribution schemes.

In homogeneous wireless sensor environment all sensor nodes have to store the large number of keys which may lead poor resilience to node capture attack. In heterogeneous wireless sensor environment the given schemes [3, 17, and 18] uses the

GPS unit to communicate to location to the cluster head. This adds additional overhead to the network. So such a hybrid key distribution scheme must be proposed which can be used for long lifespan and scalable network without additional overhead of GPS unit.

5 Conclusions

In wireless sensor network, encryption and authentication services are based on the operations involving keys. So energy efficient key distribution is an important issue. In this article we present a comprehensive survey of key distribution schemes in wireless sensor network. They have common objective of trying to distribute the keys to all sensor node with efficient use of the memory, computation power with consideration of the security aspect.

Overall, key distribution techniques can be classified on network structure as homogeneity, pre-distribution of keys and deployment knowledge basis.

Finally, we have given the comparison of all the key distribution schemes. Although, many of the techniques look promising, there are still many challenges that need to be solved in future key distribution scheme in wireless sensor network like large scalability and lifespan of the wireless sensor network.

References

1. Yong, W., et al.: A survey of security issues in wireless sensor networks. IEEE Communications Surveys & Tutorials 8, 2–23 (2006)
2. Al-Karaki, J.N., Kamal, A.E.: Routing techniques in wireless sensor networks: a survey. IEEE Wireless Communications 11, 6–28 (2004)
3. Kausar, F., et al.: Key Management and Secure Routing in Heterogeneous Sensor Networks. In: IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, WIMOB 2008, pp. 549–554 (2008)
4. Habib, A.: Sensor network security issues at network layer. In: 2nd International Conference on Advances in Space Technologies, ICAST 2008, pp. 58–63 (2008)
5. Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: attacks and countermeasures. In: Proceedings of the First IEEE, International Workshop on Sensor Network Protocols and Applications, pp. 113–127 (2003)
6. Huijuan, D., et al.: Selective forwarding attack detection using watermark in WSNs. In: ISECS International Colloquium on Computing, Communication, Control, and Management, CCCM 2009, pp. 109–113 (2009)
7. Newsome, J., et al.: The Sybil attack in sensor networks: analysis & defenses. In: Third International Symposium on Information Processing in Sensor Networks, IPSN 2004, pp. 259–268 (2004)
8. Hu, Y.C., et al.: Packet leashes: a defense against wormhole attacks in wireless networks. In: Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, INFOCOM 2003, vol. 3, pp. 1976–1986. IEEE Societies (2003)
9. Kaiping, X., et al.: Security improvement on an efficient key distribution mechanism for large-scale Wireless Sensor Network. In: 2nd International Conference on Anti-Counterfeiting, Security and Identification, ASID 2008, pp. 140–143 (2008)

10. Haowen, C., et al.: Random key predistribution schemes for sensor networks. In: Proceedings of 2003 Symposium on Security and Privacy, pp. 197–213 (2003)
11. Wenliang, D., et al.: A key management scheme for wireless sensor networks using deployment knowledge. In: Twenty-Third Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2004, 597 p. (2004)
12. Ibriq, J., Mahgoub, I.: A Hierarchical Key Establishment Scheme forWireless Sensor Networks. In: 21st International Conference on Advanced Information Networking and Applications, AINA 2007, pp. 210–219 (2007)
13. Pathan, A.S.K., Choong Seon, H.: Feasibility of PKC in resource-constrained wireless sensor networks. In: 11th International Conference on Computer and Information Technology, ICCIT 2008, pp. 13–20 (2008)
14. Eschenauer, L., Gligor, V.D.: A key-management scheme for distributed sensor network. In: 9th ACM Conference on Computer and Communications Security, Washington DC, pp. 41–47 (2002)
15. Tasci, S.E., et al.: Simple and Flexible Random Key Predistribution Schemes for Wireless Sensor Networks Using Deployment Knowledge. In: International Conference on Information Security and Assurance, ISA 2008, pp. 488–494 (2008)
16. Lu, K., et al.: A framework for distributed key management schemes in heterogeneous wireless sensor networks. In: 25th IEEE International Performance, Computing, and Communications Conference, IPCCC 2006, p. 7, 520 (2006)
17. Xiaojiang, D., et al.: A Routing-Driven Key Management Scheme for Heterogeneous Sensor Networks. In: IEEE International Conference on Communications, ICC 2007, pp. 3407–3412 (2007)
18. Banihashemian, S., Bafghi, A.G.: A new key management scheme in heterogeneous wireless sensor networks. In: 2010 The 12th International Conference on Advanced Communication Technology (ICACT), pp. 141–146 (2010)