An Empirical Study on Key Management Schemes of Wireless Sensor Network

Nazmul Islam
Institute of Information and Communication Technology
Khulna University of Engineering &Technology,
Bangladesh

M. A. Moyeen
Institute of Information and Communication Technology,
Khulna University of Engineering &Technology,
Bangladesh

ABSTRACT
The ample use of Wireless Sensor Network demands highly effective security mechanism for its sound operation in any hostile environment. The security of encrypted information greatly dependents on the rigidity of underlying Key Management techniques. Hence, key management becomes the most significant issue in case of security of Wireless Sensor Networks. The purpose of this paper is to assess most significant key management schemes of wireless sensor networks *e.g.* single network-wide key scheme, pairwise key establishment scheme, random key pre-distribution and Q-composite random key pre-distribution scheme. The overall analysis is performed based on a number of criteria such as: loaded key utilization, resource consumption and rigidity against node capture. Besides, to identify the best one, a result based comparison among the schemes is also presented.

Keywords
Wireless sensor network, key management, security, performance evaluation.

1. INTRODUCTION
Sensor technology is marked as one of the world's emerging technology by recent technological review [1]. The deployment of Wireless Sensor Networks (WSNs), which usually consist of plenty of small autonomous devices called sensor nodes, has been accelerated by the progression in sensor network technology. Due to cost effectiveness, the wireless sensor networks are quickly gaining enormous popularity for solving world challenges [2]. The low cost sensor nodes, providing extra flexibility to deploy them as a large array in a variety of conditions, are capable of performing both military and civilian tasks [3]. For the security of this network, key management has been an important research issue as traditional heavy schemes can't be applied anymore because of node's low resource nature.

Designers should consider some major resource constraints of sensor nodes: (1) limited energy, (2) limited memory, (3) limited communication bandwidth, (4) limited communication range [4], while designing a Key Management scheme for WSNs. As WSNs are deployed in unattended and hostile regions, physical security of sensor nodes [5] can't be guaranteed. Node capture attacks; an attacker gains the control of a node in the network after deployment, become a significant threat due to the lack of physical security which can maliciously modify the node to insert wrong data and perform several attacks on the network [6]. Again, attacker may eavesdrop to critical security information such as routing protocols, data, and security keys [7]. Hence, key distribution schemes of WSNs must consider the compromised nodes as well. Besides, establishing and maintaining secure and dynamic channels among communicating nodes should be the major concern of key management schemes [8]. Moreover, efficiency demands that WSNs employ a scalable key management scheme to permit alterations in the size of the network [9]. Key management schemes should provide their features not only to small networks but also to larger ones. These techniques should also be able to function well in any kind of environments and support dynamic deployment of nodes at any time. Again memory capacity of sensor nodes is usually very low [10], majority of which is occupied by a typical sensor network operating system. So the schemes should carefully utilize the remaining limited storage space for storing keys in memory, buffering stored messages etc. Apart from making the sensor networks secure, key management should introduce as less overhead as possible [11]. Normally this is a trade-off which also depends upon the application scenario.

The contents of the paper are organized as follow– Section 2 presents a brief description on wireless sensor network architecture. Section 3 describes the mechanisms of popular key management schemes: single network-wide key scheme, pairwise key establishment scheme, random key pre-distribution and Q-composite random key pre-distribution scheme. Section 4 illustrates the experimental results with a discussion on the result that reveals the efficient scheme among these four for wireless sensor network. Finally, section 5 concludes the paper with future research directions.

2. WIRELESS SENSOR NETWORK ARCHITECTURE
Wireless Sensor Networks can have hierarchical or distributed structures as shown in Figure 1. In hierarchical networks as shown in Figure 1(a), there is a chain of command among the sensor nodes: base stations, group heads and member nodes. A base station is typically a powerful storage/data processing center, gateway to another network, or works as a user interface. Base stations collect information from nodes, carries out expensive operations and organize the network. Base stations are considered to be trusted and temper resistant and responsible to register nodes prior deployment. Group heads, usually more powerful than member nodes, are deployed around the surveillance area each of which can act as a member under another group leader. This structure allows sensor network to monitor a larger area beyond the transmission range of the base station. Each leader maintains a group comprising several member nodes. Together with members a group leader monitors a pre-assigned area and transmits data to the base station. Data collected by the member nodes may transmitted through the group leaders. Data flow in such networks can be: (i) pairwise (unicast) among member nodes, (ii) group-wise (multicast) within a group of nodes, and (iii) network-wise (broadcast) from base stations to all nodes.

Distributed architecture of WSN is illustrated in Figure 1(b) where there is no fixed infrastructure and network topology is unknown before deployment. Nodes are spread randomly all over the monitoring area. Once deployed, each nodes scans its coverage area to find out its neighbors. Data flow in such network is similar to data flow in hierarchical network with a difference that network-wise (broadcast) transmission can be made by every nodes.

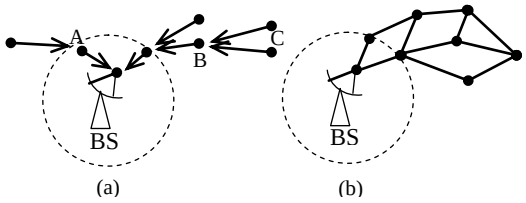


Fig 1: (a) Hierarchical architecture with base station BS, group leaders A and B, members B and C. (b) Distributed architecture with base station BS and member nodes.

3. KEY MANAGEMENT SCHEMES

This section explains the key management schemes that are evaluated in this paper. Single network-wide key and pairwise key schemes are straightforward and easy to understand, hence they are explained briefly. Random key pre-distribution schemes on the other hand are explained in detail.

3.1 Single Network-wide Key

Single network-wide key management scheme starts with a single key preloaded into all the nodes of the network. Every node in the network utilizes the same key for message encryption and decryption [4] [8]. As single key is stored in the node's memory, a minimum storage is occupied and there is no requirement of complex protocols to perform key discovery or key exchange since all the nodes in communication range can transfer messages using the shared key. However, there is a major security loophole in this scheme. If one of the sensor node is compromised, the communication security of the network collapses as adversary obtains the network wide shared key. Hence it is wise for neighboring sensor nodes to establish pairwise keys just after the network deployment.

3.2 Pairwise Key Establishment Scheme

This scheme offers many additional features including node-to-node authentication and resilience to node replication. In a network of n nodes, every node stores n–1 keys *i.e.* one for each of the other nodes in the network, so that each node can communicate with all the nodes in its communication range. A compromised node, in this scheme, can conceal information about other nodes that are not in direct communication which provides more rigidity against network capture and thus minimizes the chance for node replication [12]. However, memory overhead of this scheme is significantly higher than single network wide key approach. Since each sensor node maintains a distinct pairwise key for every other node in the network, the pairwise key approach is not scalable for large WSNs.

3.3 Random Key Pre-distribution Scheme (Basic scheme)

Random Key Pre-distribution Scheme, proposed in [13], is divided into three stages: key pre-distribution, shared-key discovery, and path-key establishment.

Key pre-distribution stages: In this stage, initially a large key pool of S keys and their corresponding identifiers are generated. k keys along with identifiers are drawn randomly from the key pool of size S and pre-distributed into each node's key ring. Trusted nodes from the network are defined as controller nodes. Key identifiers of the key ring and sensor identifiers of controller nodes are stored to get proper information about member nodes and controller nodes. Few keys are used to ensure that two nodes share a common key with certain probability, thus this scheme saves more space by storing small amount of keys.

Shared-key discovery stage: After initialization of nodes in key distribution stage nodes are deployed to their corresponding places defined by the application type *e.g.* war zone, hospital, forests etc. Upon deployment, nodes with shared keys establish connection among them. In a simplest manner shared key discovery can be done by broadcasting each nodes identifier list to other node in the network. If a node finds that it shares a common key with another node then it can start communication with that node using that shared key. Traffic analysis attack [14] is still possible for this simplest technique. To overcome this limitation, another approach of getting proper shared key would be using public key crypto-techniques where a challenge α is placed to other node with encryption like $E_j(\alpha)$. Nodes capable of decryption of $E_j(\alpha)$ with proper key will be able to use shared key defined by challenge α.

Path key establishment stage: Two nodes having shared key are said to have path in between them. In this stage a path is established, if required, between two nodes if there is no shared key found in their key list. Say node P wants to communicate with node R but they lacks a shared key. In this circumstance, P sends a message to node D encrypting with the common shared key between node P and node D denoting its willingness to communicate with node R. Node D acting like a controller node generates a pairwise key $L_{P,R}$ for node P and R. Node P and R can now communicate securely with that shared key. There is no security breach raised due to this process as request and response messages are shared with common shared key between controller node and the normal nodes.

Key revocation: Conciliation of any sensor node demands all the information associated with that node to be removed from the network especially the keys that are shared by the other nodes. The controller nodes take the responsibility to handle the node compromise issues by broadcasting a message. The message, signed and encrypted by controller node, includes a list of key identifiers of the compromised nodes key ring. After receiving the message, nodes delete the entries that corresponds to the decrypted verified identifiers of the message. As only few keys are removed from the network, it does not incur much communication overhead.

According to [13], only 75 keys are to be stored in the memory of a node with probability of p=0.5 for a key pool of 10,000 keys. They have also shown that only 250 keys are enough to be stored in a node's memory even though key pool size is enhanced by 10 times. In case of larger network this scheme can be useful due to its flexibility, scalability and smaller storage required for the keys. But this basic scheme doesn't provide node to node authentication which indeed necessary to resist node replication attack.

3.4 Q-composite Random Key Pre-distribution Scheme

Q- composite random key pre-distribution scheme, a variation of random key pre-distribution scheme, enhances the security and resilience of the network against node capture attacks. Here, in order to establish a secure communication link, a sensor node pair must share at least q keys where q is a system parameter and $q>1$. Q-composite scheme provides security under small scale attacks but becomes vulnerable under large scale attacks. The major challenge of this scheme is to select an optimal value for q while ensuring the security. If the amount of overlapping keys between two nodes is large (*i.e.*, large value of q), it becomes harder for an adversary to break the communication link, at the same time this means that by compromising a small amount of sensor nodes the adversary can gain a large part of key pool that is used by sensor nodes. At the beginning of the process each node is loaded with k random keys from a key pool of size S($k<S$). After deployment, each node tries to find common keys by asking other nodes in range to broadcast their key identifiers or by using Merkle Puzzle [15] in shared key discovery phase. In turn, a new communication key is generated as the hash of q' ($q' \geq q$) shared keys. Here, key pool size S is the critical parameter as the probability of distributing common keys between any two nodes is decreased if key pool size S becomes larger. On the other hand, in case of smaller S, adversary can gather more information by capturing only a few amount of nodes. Let $p(i)$ be the probability that any two nodes have exactly i keys in common. Any given node has $\binom{|S|}{m}$ different ways of picking its m keys from the key pool of size $|S|$. Hence, the total number of ways for both nodes to pick m keys each is $\binom{|S|}{m}^2$. Now, if the two nodes have i keys in common, there are $\binom{|S|}{i}$ ways to pick the i common keys. Which implies that, there remain $2(m-i)$ distinct keys in the two key rings that have to be picked from the remaining pool of $|S|-i$ keys and the number of ways to do this is $\binom{|S|-i}{2(m-i)}$. Again the $2(m-i)$ distinct keys can be distributed $\binom{2(m-1)}{m-i}$ ways between the two nodes equally. Hence the total number of ways to choose two key rings with i keys in common is the product of the aforementioned terms. Thus, the probability that any two nodes have exactly i keys in common is $p(i) = \binom{|S|}{i}\binom{|S|-i}{2(m-i)}\binom{2(m-1)}{m-i} \div \binom{|S|}{m}\binom{|S|}{m}$.

4. EXPERIMENTAL ANALYSIS

To evaluate the security and performance of the key distribution schemes, some important metrics such as– key utilization, resource consumption and resilience against node capture have been taken into consideration in this article. Here, key utilization shows the ratio of loaded key and used key for establishing connection with neighbors in the network. Greater key utilization ensures lesser memory wastage. As memory and power are the main concern in wireless sensor networks, they are considered as resources to evaluate the schemes in this paper. A key management scheme should be efficient in terms of resource consumption. The greater the key used for connection establishment the greater memory is required. Also, a key management scheme with high communication overhead consumes more battery power. Moreover, WSNs deployed in hostile regions is always vulnerable to physical attack. Hence, key management schemes must secure as much as information of the network from adversaries while node is compromised.

4.1 Environment Setup

The experiments over the key management schemes, described in this paper, are executed in an environment that consists of 32 bit windows machine (windows 7), Core i3 3.06 GHz CPU with 2048MB of RAM and technical computing language Matlab is used for simulation purpose. During simulation, common time requirements for message transmission in every scheme are abstained from consideration. The simulations were performed for a network of 50 nodes and the key pool size is chosen to be 100 and key ring size is set to 3 for both random key pre-distribution and Q-composite schemes. Power consumption is assumed proportional to the communication overhead and node's memory is assumed to be 1MB. Moreover, nodes are distributed randomly throughout the simulated area with an uniform radio range of 5 units.

4.2 Results and Discussion

The key utilization rate of the described key management schemes for a network with 50 nodes is presented in Figure 2. In single network-wide key scheme, since there is an active sole key in the network, each node can communicate with other nodes that fall into its range making a full utilization of the loaded key in its memory which is also shown in Figure 2 with loaded and utilized key ratio 1 *i.e.* yielding utilization factor 1. In pairwise key establishment scheme, the connectivity among the nodes is high similar to the single network-wide key scheme as each node carries keys for every other nodes in the network. But due to the nodes radio range, only a limited number of keys should be utilized to establish a secure communication with neighboring nodes. The assumption is supported by the experiment (Figure 2) with only 3 keys in utilization on average while 49 are loaded yielding the utilization factor at 0.06 *i.e.* 6% of the total loaded keys are utilized by a typical node. In random key pre-distribution scheme a node used 57% keys to achieve $p \approx 0.71$. Similarly, in Q-composite random key pre-distribution scheme the same node showed 21% secure connectivity rate using same amount of keys as before.

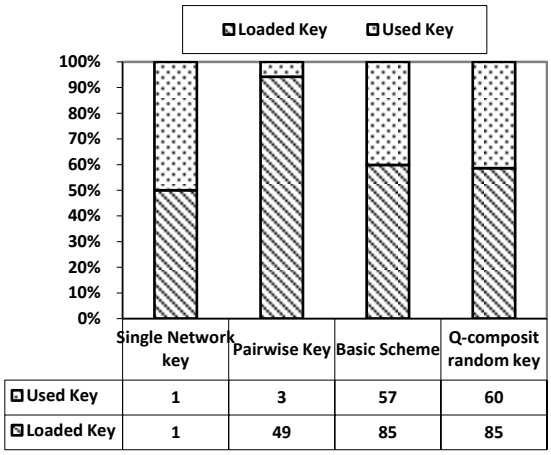
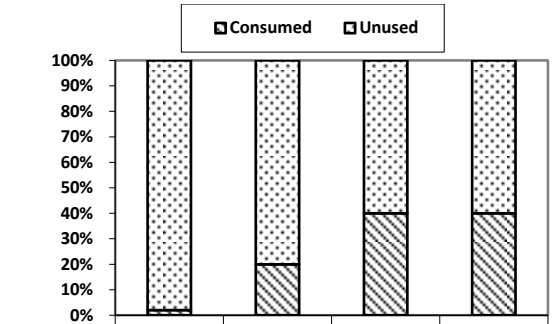


Fig 2. Loaded key to utilized key ratio.



	Single Network key	Pairwise Key	Basic Scheme	Q-composit random key
Unused	98	80	60	60
Consumed	2	20	40	40

Fig 3. Resource consumption in network establishment

Figure 3 presents the resource consumption of each key management for a network of 50 nodes. The results shows that single network-wide key scheme uses only 4 bytes of memory which is the size of one key. Moreover, there is no power consumption for communication overhead as a single key to all nodes is assigned before network deployment. In pairwise key establishment scheme, since each sensor node is loaded with a distinct key for every other node in the network, this scheme's memory overhead per node is 196 bytes. Basic and Q-composite schemes on the other hand employ 3 keys per sensor node resulting only 12-byte memory overhead. But random key pre-distribution schemes are more power consuming in terms of communication than pairwise key establishment scheme as each node has single key in pairwise key establishment scheme while in the random key pre-distribution schemes each node has number of keys equal to the ring size of the node.

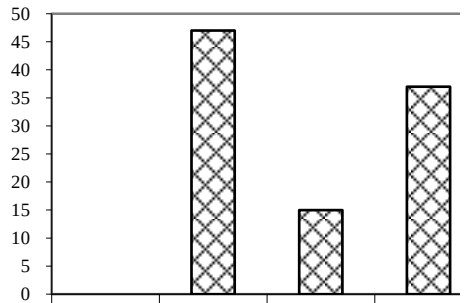
Figure 4 presents the rigidity of the schemes against node capture. If a sensor node's secret keys are revealed, it is assumed that sensor node is also captured. From the figure it is seen that, when a node is captured, pairwise establishment scheme is the most efficient and resistant scheme while single network-wide key scheme loses all nodes in the network. The simulation results also show that Q-composite scheme is more rigid compared to basic scheme.

5. CONCLUSION AND FUTURE WORKS

WSNs are promising solutions for many applications and security is a vital requirement for these networks. This paper explains and evaluates some important key management schemes in wireless sensor networks. Namely, single network-wide key scheme, pairwise key establishment scheme, random key pre-distribution and Q-composite random key schemes are evaluated with simulation results and comparisons. The results show that random key pre-distribution techniques are the most suitable key management schemes among others for wireless sensor networks in terms of performance and security. The future research directions may involve comparing more key management schemes using different metrics and larger network sizes.

6. ACKNOWLEDGMENTS

The Authors are willing to express their profound gratitude and heartiest thanks to all the researchers in the field of wireless sensor network's security, who have made their research works easy to accomplish.



	Single Network key	Pairwise Key	Basic Scheme	Q-composit ra key
Working nodes	0	47	15	37

Fig 4. Rigidity against node capture.

7. REFERENCES

[1] Raghavendra, C.S., Sivalingam, K.M. and Znati, T. eds., 2006. Wireless sensor networks. Springer.

[2] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. Communications magazine, IEEE, 40(8), 102-114.

[3] El-Aasser, M., & Ashour, M. (2013, January). Energy aware classification for wireless sensor networks routing. In Advanced Communication Technology (ICACT), 2013 15th International Conference on (pp. 66-71). IEEE.

[4] Xiao, Y., Rayi, V. K., Sun, B., Du, X., Hu, F., & Galloway, M. (2007). A survey of key management schemes in wireless sensor networks. Computer communications, 30(11), 2314-2341.

[5] Barbareschi, M., Battista, E., Mazzeo, A., & Venkatesan, S. (2014, August). Advancing WSN physical security adopting TPM-based architectures. In Information Reuse and Integration (IRI), 2014 IEEE 15th International Conference on (pp. 394-399). IEEE.

[6] Ho, J. W. (2010). Distributed detection of node capture attacks in wireless sensor networks. INTECH Open Access Publisher.

[7] Hartung, C., Balasalle, J., & Han, R. (2005). Node compromise in sensor networks: The need for secure systems. Department of Computer Science University of Colorado at Boulder.

[8] Zhang, J., & Varadharajan, V. (2010). Wireless sensor network key management survey and taxonomy. Journal of Network and Computer Applications, 33(2), 63-75.

[9] Bechkit, W., Challal, Y., Bouabdallah, A., & Tarokh, V. (2013). A highly scalable key pre-distribution scheme for wireless sensor networks. Wireless Communications, IEEE Transactions on, 12(2), 948-959.

[10] Ruj, S., Nayak, A., & Stojmenovic, I. (2013). Pairwise and triple key distribution in wireless sensor networks with applications. Computers, IEEE Transactions on, 62(11), 2224-2237.

[11] Abdallah, W., Boudriga, N., Kim, D., & An, S. (2014, February). An efficient and scalable key management mechanism for wireless sensor networks. In Advanced

Communication Technology (ICACT), 2014 16th International Conference on (pp. 687-692). IEEE.

[12] Sun, D., & He, B. (2006). Review of key management mechanisms in wireless sensor networks. Acta Automatica Sinica, 32(6), 900.

[13] Eschenauer, L., & Gligor, V. D. (2002, November). A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM conference on Computer and communications security (pp. 41-47). ACM.

[14] Di Ying, B., Makrakis, D., & Mouftah, H. T. (2014). Anti-traffic analysis attack for location privacy in WSNs. EURASIP Journal on Wireless Communications and Networking, 2014(1), 1-15.

[15] Merkle, R. C. (1978). Secure communications over insecure channels. Communications of the ACM, 21(4), 294-299.