Secure and Efficient Key Management Protocol (SEKMP) for Wireless Sensor Networks

Majid Alshammari and Khaled Elleithy
Department of Computer Science and Engineering
University of Bridgeport
Bridgeport, CT 06604
maalsham@my.bridgeport.edu; elleithy@bridgeport.edu

ABSTRACT
Wireless sensor networks (WSNs) are used in the many critical applications, such as, military, health, and civil applications. Sometimes such applications require that the WSNs to be randomly deployed in inaccessible terrains such as a remote territory. As a result, the sensors are left unattended and become a potential target for an adversary. Therefore, we propose a highly Secure and Efficient Key Management Protocol for WSN, called SEKMP. The proposed protocol (SEKMP) adapts a new key management approach by leveraging the advantages of asymmetric cryptography and employs them in a very efficient way for delivering the session key to sensor nodes.

Categories and Subject Descriptors
E.3 [Data Encryption]: Public key cryptosystems; C.2.1 [Computer-Communication Networks]: Network Architecture and Design – *Wireless communication*

Keywords
Wireless sensor networks.

1. INTRODUCTION
Wireless sensor networks (WSN) is a growing area, and today become involved in variety of applications due to the nature of sensors nodes that are small in size and cost effective [1]. WSN in inaccessible terrains is usually left unattended. As a result, they become an easy target for an adversary. In such environments, the major security concern of WSN is the key management protocol. Thus, there are varieties of protocols in literature that utilize one or more of the following schemes: symmetric, asymmetric, or quantum cryptography for addressing the security of key management in WSN. However, the direct application of these schemes is not the best choice when it comes to limited-resource environments such as WSN. With this in mind, we came up with a very Secure and Efficient Key Management Protocol for WSN, called SEKMP. The proposed protocol (SEKMP) adapts a new key management approach by inheriting the advantages of asymmetric cryptography and employs it in very efficient way for delivering the session key to sensor nodes.

Symmetric-based key management protocols are considered more resource-efficient than Asymmetric-based key management. The downsides of these protocols are: 1) maintaining a large number of keys, 2) or dependency on intermediary nodes for the keys distribution. For example, [2] and [3]. Asymmetric-based key management protocols proved to be secure in literature, and thus, they are one of the best protocols for the key distribution. The downside is, the direct application of these protocols in WSN leads to have many keys, and as a result, affecting the protocol performance. For example, in [4] the sink node must maintain n keys with sensor nodes. Where n is the number of nodes.

ANCS'14, October 20–21, 2014, Los Angeles, CA, USA
ACM 978-1-4503-2839-5/14/10.
http://dx.doi.org/10.1145/2658260.2661775

2. THE PROPOSED PROTOCOL
SEKMP includes three phases: Pre–deployment phase, Key distribution phase, and Key refreshment phase. Table 1 shows the notations used in the proposed protocol.

Table 1. Notations

Notation	Description
N	Number of nodes.
PU_S	Public key used in the sink node.
PR_N	Private key used in each node.
K_S	Session key used to encrypt the communication.
C	Ciphertext.
M	Plaintext.
E_K (X)	Function for Encrypting X with K.
D_K (X)	Function for Decrypting X with K.

2.1 Pre-deployment phase
In pre-deployment phase, a pair of keys, called public (PU_S) and private (PR_N) key is generated for the WSN. The public key (PU_S) is assigned to the sink node, whereas, the private key (PR_N) is assigned to the sensor nodes. Afterwards, the sink node has the public key (PU_S), and each sensor of the WSN has a copy of the private key (PR_N). Furthermore, building Wireless Sensor Network of N nodes requires two keys only, one for the sink node and the other one for the sensors nodes.

2.2 Key distribution phase
After the sensor nodes have been deployed, the sink node generates a random session key (K_S), and then encrypts the session key by using its key, the public key (PU_S). Then, the sink node broadcasts the following cipher message $C = E_{PU_S}(K_S)$ to its neighbors. These neighbors broadcast the same cipher message to their neighbors if any, in multi-hop fashion until all sensor nodes get the cipher message. Since all the sensor nodes already have the private key (PR_N), they can decrypt the cipher message $C = E_{PU_S}(K_S)$ as, $K_S = D_{PR_N}(C)$. In the end, the entire nodes securely receive the session key (K_S). Figure 1 shows the key distribution phase.

2.3 Key refreshment phase
In the key refreshment phase, the sink node can generate a new session key (K_S) on time-basis (e.g. generating a new session key every 24 hours), or on event-basis, (e.g. generating a new session

key whenever a node detects a specific event) based on the desired application, and then securely broadcasts it to the all sensor nodes as it does in the key distribution phase. The key refreshment phase makes the proposed scheme more secure because of its flexibility of generating a new session key at any time and for any reason.

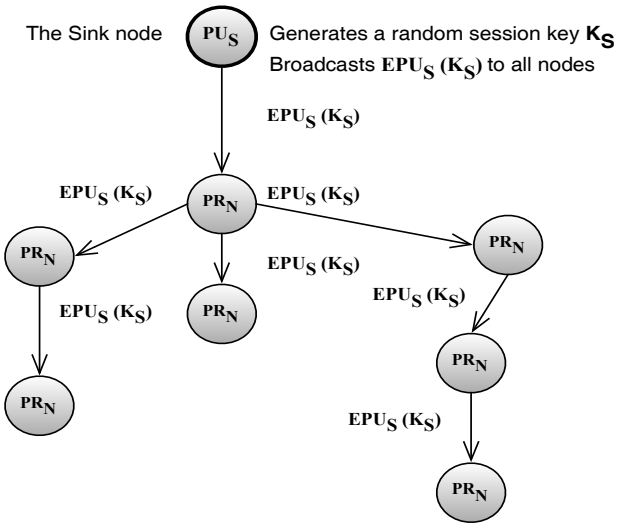

Figure 1. key distribution phase.

3. PROPOSED PROTOCOLS ANALYSIS

3.1 Security analysis

In this section, the security of the proposed protocol (SEKMP) is analyzed and investigated based on the following security services: Confidentiality, Integrity, and Authenticity.

3.1.1 Confidentiality

The proposed protocol (SEKMP) assures the confidentiality of the communication among sensors nodes by using a session key (K_S). This session key is securely delivered by utilizing the asymmetric encryption properties.

3.1.2 Integrity

The integrity is achieved in the proposed protocol by encrypting the traffic by the authorized nodes to prevent data modification. Also, the protocol can employ Message Authentication Codes (MAC) to guarantee that the message has not been altered.

3.1.3 Authentication

This security service is assured by using a pair of keys, called public (PU_S) and private (PR_N) key. Since the sink node is the only node that has the public (PU_S) key, it encrypts the session key (K_S) by the public key and broadcasts it to the sensor nodes. Once the sensor nodes successfully decrypt it by the private key (PR_N), this authenticates the sink node to the sensor nodes in the network and proves that the session key (K_S) is sent by a trusted source.

3.2 Performance analysis

In this section the performance of proposed protocol (SEKMP) is analyzed according to Efficiency, Connectivity, Scalability, and Flexibility.

3.2.1 Efficiency

The efficiency of the proposed protocol (SEKMP) is achieved by using a small number of keys compared to other protocols such as [2], [3], and [4]. It also provides an extremely secure key management protocol in the same time. As a result, SEKMP preserves the energy of the sensors. Table 2, represents the number of keys being used by the sink node/KDC, and each sensor node in SEKMP, [2], [3], and [4].

Table 2. Numbers of keys

Scheme/protocol.	Number of keys in the sink node.	Number of keys in each sensor node.
SEKMP	1	1
[2]	$\sqrt{n}$	$\sqrt{n}$
[3]	n x $\lfloor n/2 \rfloor$	n -1
[4]	n	2

3.2.2 Connectivity

Connectivity of the proposed protocol is considered high because the protocol ensures that each node would receive a session key (K_S) by broadcasting an encrypted message contains that session key.

3.2.3 Scalability

The proposed protocol is able to maintain the security of the wireless sensor as the network expands, and it can be achieved by adding N nodes with an assigned private key (PR_N).

3.2.4 Flexibility

The proposed protocol is flexible due the fact that a node can be added or removed easily; even the sink node can be replaced without affecting the security of WSN. For example, a sink node can be added after it gets assigned with the public key (PU_S). Also with the same approach, a sensor node can be added after it is assigned with the private key (PR_N).

4. CONCLUSIONS

The SEKMP protocol adapts a new key management approach by leveraging the advantages of asymmetric cryptography properties and employs them in a very efficient way for delivering the session key to sensor nodes. We have simulated and compared SEKMP to existing protocols in literature in terms of the number of keys being used. Based on the simulation results, SEKMP is protocol is more efficient than those protocols. Thus, we believe that adapting SEKMP protocol addresses several security challenges of the key management in WSNs.

5. REFERENCES

[1] I. F. Akyildiz and M. C. Vuran, *Wireless sensor networks* vol. 4: John Wiley & Sons, 2010.

[2] H. Chan and A. Perrig, "PIKE: Peer intermediaries for key establishment in sensor networks," in *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, 2005, pp. 524-535.

[3] L.-C. Wuu, C.-H. Hung, and C.-M. Chang, "Quorum-based key management scheme in wireless sensor networks," presented at the Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication, Kuala Lumpur, Malaysia, 2012.

[4] Y. Zhang, "The scheme of public key infrastructure for improving wireless sensor networks security," in *Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference on*, 2012, pp. 527-530.