Multi-Level Dynamic Key Management for Scalable Wireless Sensor Networks with UAV

Ozgur Koray Sahingoz

Abstract Wireless Sensor Networks (WSNs) are more vulnerable to security attacks than wired networks because of their wireless and dynamic nature. In today's WSNs, the sensor nodes act not only as routers but also as communication endpoints, and they are also responsible for the security of the messages. Therefore, it is important to define whether an incoming message originates from a trustworthy node or not. The main solution for this is the usage of cryptographically signed messages. There are two main classifications for signing messages: namely *symmetric* and *asymmetric* algorithm based cryptography. In the asymmetric key cryptography, public/private key pairs are used to encrypt and decrypt messages. However, it can cause severe computational, memory, and energy overhead for the nodes. On the other side, symmetric key cryptography is superior to asymmetric key cryptography in terms of speed and low energy cost, but at the same time, it needs to design an efficient and flexible key distribution schemes for improving system performance. In this paper, it is aimed to set a multi-level dynamic key management system for WSNs with the aid of an Unmanned Aerial Vehicle (UAV) as a key distribution and coordination center for asymmetric keys. Public keys of the sensor nodes are dispatched by UAVs and symmetric keys set with these key combinations. Evaluation results show the proposed system is scalable, and its performance is considerably better than single asymmetric key management systems

Keywords WSN · Security · Encryption · Symmetric key · Asymmetric key

O. K. Sahingoz (✉)
Turkish Air Force Academy, Computer Engineering Department, 34149 Istanbul, Turkey
e-mail: sahingoz@hho.edu.tr

Y.-H. Han et al. (eds.), *Ubiquitous Information Technologies and Applications*,
Lecture Notes in Electrical Engineering 214, DOI: 10.1007/978-94-007-5857-5_2,

1 Introduction

As a result of the recent advances in micro-electromechanical systems wireless sensor networks have attracted much attention especially in various application areas like surveillance, target tracking, search and rescue, industrial and environmental monitoring, automation in the transportation, security, and healthcare applications [1]. Wireless sensor networks (WSNs) use small battery-operated sensor nodes consist of sensing, data processing, and wireless communicating components. Therefore, these nodes have constrained data processing capability, storage capacity, transmission range, and power capability.

Next generation sensor networks will be long-lived and highly dynamic, and they will contain multifunctional sensor nodes. Although most of the WSNs developed for application specific manner, nowadays "One deployment, multiple applications" concept is an emerging trend [2, 3]. To run multiple applications for a long time, decreasing power consumption, improving power sources and survivability of the system are challenging tasks.

As sensor networks grow in capability and are used more frequently, not only survivability but also security issues become extremely important especially in mission-critical tasks such as military applications. Thus, security needs should be taken into account at every aspect of system design. In wireless sensor networks, implementing security is a great challenge for data gathering and aggregating [4], however, constructing the physical security of wireless links is impossible because of the broadcast nature of wireless communications and uncontrolled environments.

Security can be constructed with different types of schemes [5], but generally, to provide secure communications, every message between sensor nodes should be encrypted and authenticated. Evidently, using a single shared key for the whole WSN is not a good idea because an adversary can easily obtain this key. Another approach is to preconfigure the network with a shared unique and symmetric key between each pair of nodes. However, this mechanism does not scale well. In a network, which consists of n nodes, each node should store $n - 1$ keys and most of these keys are not even used once. At the same time, adding new sensor nodes is also impossible with this approach. Public-key cryptography (or asymmetric cryptography) is another option for encryption. Although, this approach can set up a secure key with any other node in the network, many current sensor nodes have constrained computational power and battery; this makes the usage of public-key cryptography for encryption too expensive in terms of system overhead.

However, encrypting the data is relatively the easiest part; especially for asymmetric cryptography, key management is the hardest part. Therefore, security solutions have to depend very much on the use of strong and efficient key distribution and management. To establish and maintain secure channels, the key management mechanism is responsible for key generation, key distribution, and key maintenance among sensor nodes. It should also enable sensor networks scaling to a large number of nodes. Numerous key management schemes have been proposed for sensor networks.

In this work, a multi-level dynamic key management mechanism for wireless sensor network is established. In one side, this approach allows low-level security for less important data, like sensed data, thus saving energy. In the other side, it allows higher levels of security for more sensitive data, like setting up a symmetric key between communicating nodes, thus consuming more energy. For the dynamic and scalability of the system, UAVs are used as a key distribution and management center.

This paper is structured as follows: In Sect. 2, the related works on this topic are presented. Section 3 introduces system design details and evaluations of the system are explained in Sect. 4. In Sect. 5, the paper is concluded and outlined directions for future researches.

2 Related Works

Key management and security features of the sensor networks are analyzed in some surveys in the literature [6, 7]. There are two main classifications of key management architectures; namely symmetric and asymmetric algorithm based architectures. If the encryption key is identical with the decryption key, this is called as a symmetric key algorithm. If different keys are used for encryption and decryption, this is called as an asymmetric key algorithm. An asymmetric key algorithm, unlike from symmetric key algorithms, does not require a secure initial exchange of one or more secret keys between communicating nodes.

Due to the constraints in sensor nodes, most of the researches preferred *symmetric key cryptography* in designing their WSN security. In a key pre distribution scheme, before deploying the nodes, different key or key information are distributed to the sensor nodes, and then any two nodes can establish a connection by getting the ID of each other. As a result of not requiring a KDC node, comparing to KDC based solutions; this solution meets the requirements of wireless sensor network better [8].

There are two main key pre-distribution schemes. Using a single network-wide key scheme is the simplest form of pre distribution scheme and the key is preloaded into all sensor nodes before deployment process. After deployment, every sensor node uses this key for secure communication. Although it requires minimal storage and avoids complex key management protocols, an adversary can easily obtain this key, security of the system is collapsed. On the other hand, some researches prefer the pairwise key establishment scheme [9] in which key pre distribution is done by assigning each node a unique pairwise key of the other nodes. For example if the WSN contains 20,000 nodes, then 19,999 pairwise keys should be stored at each node.

For large sensor networks, it is not a feasible solution to store all unique keys of other nodes. Moreover, these schemes do not enable scalability for the sensor networks. Therefore, the key distribution schemes based on symmetric key cryptography are not perfect. It requires a Key Distribution Center (KDC) for

enable scalability and enhance the security. With the usage of KDC, an efficient and flexible key distribution schemes need to be designed.

Asymmetric cryptography, in which a pair of keys is used to encrypt and decrypt a message, has been accepted as one of the most successful mechanisms for providing fundamental security requirements since its birth more than 20 years. Although most researches did not prefer the public key cryptography in WSNs as a result of the constraints on computation and power consumption of sensor nodes, recent progress in sensor hardware and cryptography has shown that public key cryptography may be suitable for sensor networks [10, 11].

RSA and elliptic curve cryptography (ECC) are generally used to implement asymmetric cryptosystems. The attraction of ECC can provide the same level and type of security as RSA but with smaller key size, thereby reducing processing and communication overhead. Wander et al. report that usage of these mechanisms is possible by using 8-bit CPUs and ECC demonstrates a performance advantage over RSA [12].

3 System Design

Since most of military missions are performed in hostile areas, sensor nodes are usually scattered randomly over the target area especially via aerial deployment from aerial vehicles. In this study, it is aimed to develop a secure WSN system which minimizes resource consumption and maximizes security performance.

This system, as shown in Fig. 1, consists of many nodes, which are distributed into a large area and one (or more) unmanned aerial vehicle, which is the Mobile Certification Authority (MCA) and coordination center of the system.

In this type randomly scattered deployments, setting up a secure communication is challenging and important task. Security services can be ensured by cryptography, and selecting the most appropriate cryptographic method is one of the vital parts of the system. The selected method should meet the constraints of sensor nodes like power consumption, code size, data size, and processing time. Due to the constraints in sensor nodes, keys are used as pairwise keys, which are symmetric and shared between neighboring nodes, for maintaining secrecy and resilience to attacks or failures.

In large-scale deployment scenarios, sensor nodes are scattered randomly, and there is no prior knowledge about network configuration. Therefore, pairwise keys can be distributed before deployment. While the size of the network expanding, a large number of keys are needed to be managed in order to encrypt and authenticate key for all other nodes in the WSN System.

To solve this problem some researches focused on Diffie Hellman key exchange on sensor nodes. This mechanism provides a shared secret key between two parties that have no prior knowledge of each other by communicating over an insecure communications channel. Because of the usage of insecure communications channels, this mechanism does not be preferred much.

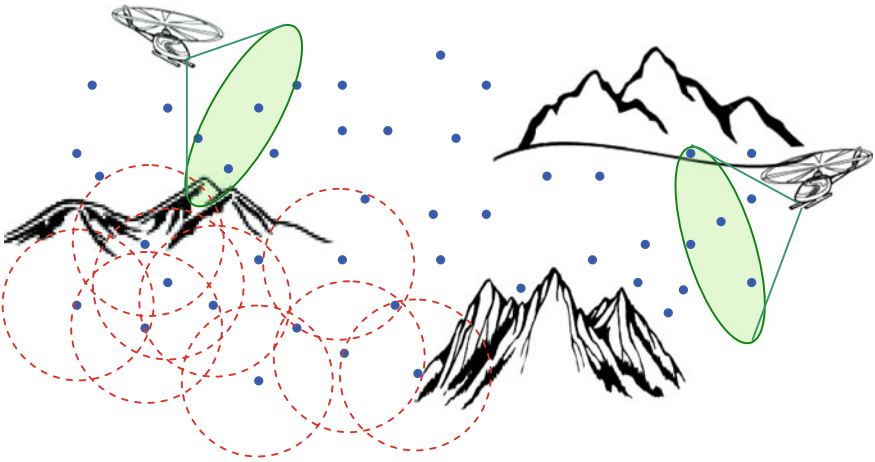

Fig. 1 Multi-Level Dynamic Key Management System for WSNs

On the other hand, public key cryptography can provide some of the strongest techniques against most vulnerabilities, however, it encounters with storage problems. In this project, it is aimed to store only the neighbors' public keys in the sensor nodes.

Once the sensor nodes have authenticated each neighbours, they can use public-keys for ensuring secure communication to agree on a pairwise session key. This symmetric session key is used for efficient symmetric cryptography in the remainder of the communication.

For dynamically managing this symmetric key infrastructure, communicating parties should change pairwise keys periodically, on demand or on detection of capture keys. By this way, network survivability is enhanced, and captured keys are replaced in a timely manner.

Key Distribution and Encryption Model of the system is depicted in Fig. 2. The main components and operations of the mode are as follows;

- Node A and Node B are two communicating sensor nodes in the WSN System.
- MCA is a mobile node within an ad hoc network, and it is selected to provide distributed key management center's functionality (in the UAV)
- K_{AB} is the communication pairwise keys between nodes A and B
- $\{M\}\ Pub_A$ denotes the encryption of message M with Public Key of node A

Setting up a symmetric key with usage of public keys of the neighbor nodes is achieved with the following key agreement protocol:

Step 1 A sensor node (Node A) broadcast a message, which contains its ID (ID_A) to its neighbors

Step 2 Each neighbor (Node B and others) should obtain the Public Key of Node A from MCA,

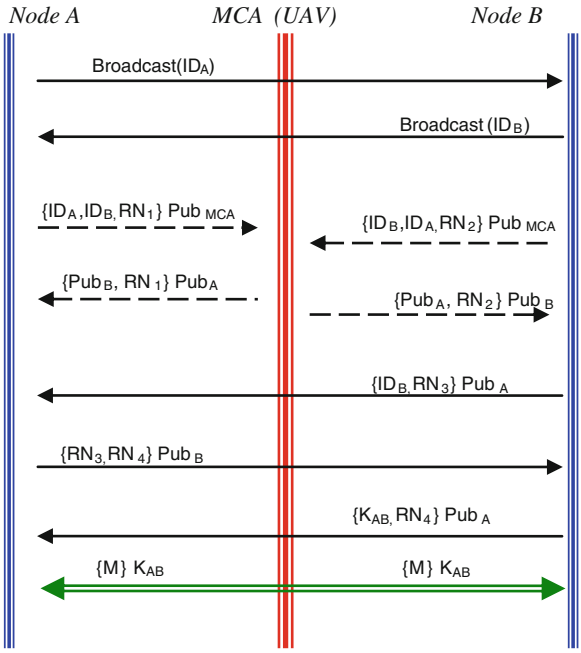

Fig. 2 Key distribution and encryption model of the system

Step 3 Node B uses Node A's public key to encrypt messages which contain its identifier (ID_B) and a random number (RN_1), which is used to identify this transaction

Step 4 Node A sends a message to Node B encrypted with Pub_B and containing B's random number (RN1) as well as a new random number generated by Node A (RN_2)

Step 5 Node B selects a secret key KAB and returns this and RN2, which are encrypted using Pub_A, to assure A that its correspondent is B

Step 6 The communicating parties are agreeing on a pairwise key and they can use this for secure communication

3.1 Development Platform

Sun SPOT [13] motes are used to develop our secure WSN system. This platform runs Java code on the motes, and the system is achieved through the implementation of a Java Virtual Machine (VM) known as Squawk. Each mote consists of a rechargeable (via USB) battery unit, 180 MHz 32-bit ARM920T microprocessor, Chipcon/Texas Instruments CC2420 radio transceiver, 512 kB of RAM and 4 MB of flash memory and three main sensors which detect change in accelerometer, light and temperature.

3.2 Java Based Development

Most of the sensor network platforms are developed with nesC programming language, which is developed for networked embedded systems to simplify application development and reduces code size.

The main advantage of Sun SPOTs is the usage of Java language, compared to TinyOS based motes, which use nesC. Therefore, development of Sun SPOT applications is easier with regard to the aspect of programming and deployment.

4 Performance Evaluation

Wander et al. [12] presented energy analysis of two PKI schemes; ECC and RSA. They illustrated significant advantages to using ECC over RSA, through implementation and analysis. As shown in Table 1, it is known that ECC can provide the equivalent level of security for a key size of 160 bits as RSA can provide with 1024-bit keys [14]. Therefore, usage of ECC is a good choice for asymmetric cryptography in WSN system.

One important constraint for sensor nodes is the space requirements of the applications. Nodes have limited memory, storage capabilities and CPU speed. Therefore, sizes of the public key and private key are also an important factor for developing a Secure WSN system. As depicted in Table 2, ECC not only has less key size than RSA, but also its encrypted message size is very small [14].

Boyle and Newe [15] show that, AES uses about five times more energy than RC4 in WSN systems. As a result, it is beneficial to use ECC algorithm as the asymmetric key encryption and RC4 algorithm as symmetric key encryption algorithm for secure communication between nodes. At the same time, using

Table 1 RSA and ECC comparison

Time to break (in MIPS years)	RSA key size (in bits)	ECC key size (in bits)	RSA/ECC key ratio
10^4	512	106	5:1
10^8	768	132	6:1
10^{11}	1024	160	7:1
10^{20}	2048	210	10:1
10^{78}	21000	600	35:1

Table 2 Space Requirements

	Public Key (bits)	Private Key (bits)	Encrypted message (for 100-bit message) (bits)
1024 bit RSA	1088	2048	1024
160 bit ECC	161	160	321

secure radiostream consumes much of the limited resources of sensor nodes. Therefore, it is needed to be more careful when sending encrypted messages.

5 Conclusion and Future Works

In this paper, a practical key management framework for a large-scale distributed wireless sensor network system is presented. WSN nodes constitute a group and securely communicate with each other by symmetric encryption. As a structure of the mechanisms, this group key should be refreshed in certain intervals by help of UAVs and a more secure encryption mechanism; asymmetric encryption. Java based WSN platform is used for this proposed system, performance evaluations results shows that using ECC asymmetric encryption algorithms is the best choice for Sun SPOT nodes for setting RC4 pairwise secret keys .

As a future work, this key distribution mechanism can be expanded by using mobile agents in WSN systems. By this approach, there will be no need for UAVs to communicate with each nodes one-by-one, sending a key distribution agent to a cluster will be sufficient for key updates.

References

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A survey on sensor networks. IEEE Commun. Mag. **40**(8), 104–112 (2002)
2. Chen, M., Kwon, T., Choi, Y.: Mobile agent-based directed diffusion in wireless sensor networks. EURASIP J. Adv. Signal Process. **2007** (2007)
3. Sahingoz, O.K.: Mobility of users in sinkless wireless Sensor networks. In: International Workshop on Telecommunications-IWT 2011, Rio de Janeiro, Brazil (2011)
4. Roy, S., Conti, M., Setia, S., Jajodia, S.: Secure data aggregation in wireless sensor networks. IEEE Trans. Inf. Forensics Secur. **7**(3), 1040–1052 (2012)
5. Rasheed, A., Mahapatra, R.N.: The three-tier security scheme in wireless sensor networks with mobile sinks. IEEE Trans. Parallel Distrib. Syst. **23**(5), 958–965 (2012)
6. Chen, X., Makki, K., Yen, K., Pissinou, N.: Sensor network security: A survey. IEEE Commun. Surv. Tutor. **11**(2), 52–73 (2009)
7. Xiao, Y., Rayi, V.K., Sun, B., Du, X., Hu, F., Galloway, M.: A survey of key management schemes in wireless sensor networks. Comput. Commun. **30**(11–12), 2314–2341 (2007)
8. Huang, H.F.: A new design of efficient key pre-distribution scheme for secure wireless sensor networks. In: Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP 2007), vol. 1, pp. 253–256 (2007)
9. Chan, H., Perrig. A.: Random key predistribution schemes for sensor networks. In: 2003 IEEE Symposium on Security and Privacy, pp. 197–213 (2003)
10. Munivel, E., Ajit, G.M.: Efficient public key infrastructure implementation in wireless sensor networks. In: International Conference on Wireless Communication and Sensor Computing (ICWCSC 2010), pp. 1–6 (2010)
11. Ren, K., Yu, S., Lou, W., Zhang, Y.: Multi-user broadcast authentication in wireless sensor networks. IEEE Trans. Veh. Technol. **58**(8), 4554–4564 (2009)

12. Wander, A.S., Gura, N., Eberle, H., Gupta, V., Shantz, S.C.: Energy analysis of public-key cryptography for wireless sensor networks. In: Third IEEE International Conference on Pervasive Computing and Communications (PerCom 2005), pp. 324–328 (2005)
13. Sun Microsystems, Inc, Project Sun SPOT: Sun small programmable object technology (online). available: http://www.sunspotworld.com/. Accessed 30 May 2012
14. Current public-key cryptographic systems. In: A Certicom Whitepaper, Certicom, pp. 1–6 (1997)
15. Boyle, D.E., Newe, T.: On the implementation and evaluation of an elliptic curve based cryptosystem for Java enabled wireless sensor networks. Sens. Actuators A Phys. **156**(2), 394–405 (2009)

http://www.springer.com/978-94-007-5856-8

Ubiquitous Information Technologies and Applications
CUTE 2012
Han, Y.-H.; Park, D.-S.; Jia, W.; Yeo, S.-S. (Eds.)
2013, XIV, 914 p. 404 illus., Hardcover
ISBN: 978-94-007-5856-8