A Riskless and Secured Communication with the Help of Wireless Sensor Networks

I Surya Prabha
Associate Professor
Department of IT,
Institute of Aeronautical Engineering,
Hyderabad, India.

Abstract

Wireless sensor networks (WSNs) consists of small nodes with constrained capabilities to sense, collect, and disseminate information in many types of applications. Wireless sensor networks (WSN) have attracted significant interests from the research community in a wide range of applications such as target tracking, environment monitoring, military sensing, distributed measurement of seismic activity, and so on.As sensor networks become wide-spread, security issues become a central concern. In this paper, we identify the Security requirements of key management in WSN. The secure management of the keys is one of the most critical elements when integrating cryptographic functions into a system. An outline of hybrid cryptography, one way hash and Key infection schemes are discussed in this paper. Along the way we analyze the advantages and disadvantages of current secure schemes. Finally, we aim to provide the different techniques of efficient key management operations for secure communications in WSN.

Keywords- Security, Key management, Wireless Sensor Networks.

I.INRODUCTION

THE Internet of Things (IoT) is a novel paradigm that has received considerable attention from both academia and industry. The basic idea of IoT is the pervasive presence around us of a variety of things or objects-such as radio-frequency identification (RFID) tags, sensors, actuators, mobile phones, etc.-which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals [1]. Wireless sensor networks (WSNs) are ad hoc networks which usually consist of a large number of tiny sensor nodes with limited resources and one or more base stations.

Usually, sensor nodes consist of a processing unit with limited computational power and limited capacity. On the other hand, the base station is a powerful trusted device that acts as an interface between the network user and the nodes. WSNs have many applications, including military sensing and tracking, environment monitoring, target tracking, healthcare monitoring, and so on. A user of the WSNs can read the data received from the sensors through the base station. If we hope to read the data anywhere in the world, we need to integrate the WSNs into the Internet as part of the IoT. There are three methods to accomplish this integration, front-end proxy solution, gateway solution and TCP/IP overlay solution [2]. In the front-end proxy solution, the base station acts as an interface between the WSNs and the Internet. There is no direct connection between the Internet and a sensor node. The base station parses all incoming and outgoing information. In the gateway solution, the base station acts as an application layer gateway that translates the lower layer protocols from both networks. In the TCP/IP overlay solution, sensor nodes communicate with other nodes using TCP/IP. The base station acts as a router that forwards the packets from and to the sensor nodes. In both gateway solution and TCP/IP overlay solution, the sensor nodes can communicate with the Internet hosts directly. However, new security challenges will appear, such as setup of a secure channel between a sensor node and an Internet host that supports end-to-end authentication and confidentiality services. Note that the computational power and storage of a sensor node are limited. But an Internet host has strong computational power and storage. So we hope to design a secure communication scheme that fits such a characteristic.

To support the authenticity of public keys in the public key cryptography, there are two main infrastructures called public key infrastructure (PKI) and identity-based cryptog-raphy (IBC) [3]. In the PKI, a certificate

authority (CA) issues a certificate which provides an unforgeable and trusted link between the public key and the identity of a user by the signature of the CA. The drawback of the PKI is that we need to manage certificates, including revocation, storage and distribution. In addition, we need to verify the validity of certificates before using them. The PKI technique has been widely developed and applied in the Internet. In the IBC, a user's public key is derived directly from its identity information, such as telephone numbers, email addresses and IP addresses. Secret keys are generated for users by a trusted third party called private key generator (PKG). Authenticity of a public key is explicitly verified without requiring any certificate. The advantage of the IBC is that we eliminate the need for certificates and some of the problems associated with them. On the other hand, the dependence on the PKG who can generate all users' secret keys inevitably causes the key escrow problem in the IBC. For the WSNs, IBC is the best choice because there is no certificates problem. However, IBC is only suitable for small networks. For the Internet security, we need PKI technique.

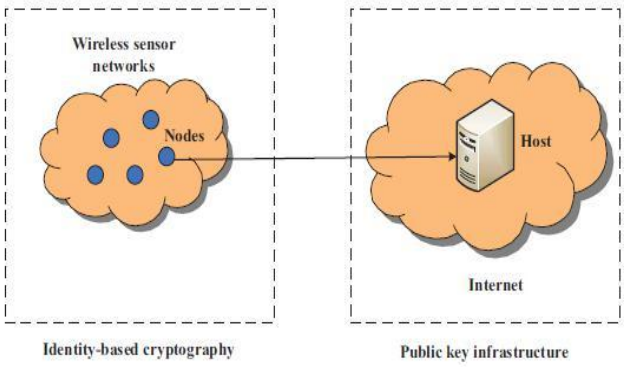

Fig. 1. Communication model for integrating WSNs into the Internet.

Motivation and Contribution

The motivation of this paper is to setup a secure channel between a sensor node and an Internet host that supports end-to-end confidentiality, integrity, authentication and non-repudiation services. In addition, we require that the IBC is used in the sensor node and that the PKI is used in the Internet host. We also require that the computational cost of sensor nodes is low. Our solution is heterogeneous online/offline signcryption (HOOSC). Concretely, we propose an efficient HOOSC scheme. We prove that the proposed scheme has the indistinguishability against adaptive chosen ciphertext attacks (IND-CCA2) under the bilinear Diffie-Hellman inver-sion problem (BDHIP) and existential unforgeability against adaptive chosen messages attacks (EUF-CMA) under the q-strong Diffie-Hellman problem (q-SDHP) in the random oracle model. Our scheme has the following characteristics:

(i) It achieves confidentiality, integrity, authentication and non-repudiation in a logical single step. (ii) It allows a sensor node in the IBC to send a message to an Internet host in the PKI. (iii) It splits the signcryption into two phases: offline phase and online phase. In the offline part, most heavy computations are done without the knowledge of a message. In the online stage, only light computations are done when a message is known.

II.KEY MANAGEMENT

The Sensor nodes cannot practically use a third party trusted server because of the high communication cost and deployment cost. The Public Key protocols involve high computation cost. Hence the Symmetric Key Cryptography involving is considered to be the better method of cryptography system in WSN. Sensor network dynamic structure, easy node compromise and self organization property increase the difficulty of key management and bring a broad research issues in this area. Due to the importance and difficulty of key management in WSNs, there are a large number of approaches focused on this area. Based on the main technique that these proposals used or the special structure of WSNs, we classify the current proposals as key pre-distribution schemes, hybrid cryptography schemes, one way hash schemes, key infection schemes, and key management in hierarchy networks, though some schemes combine several techniques.

A. KEY PRE-DISTRIBUTION SCHEMES:

In the key predistribution schemes, sensor nodes store some initial keys before they are deployed. After deployed, the sensor nodes can use the initial keys to setup secure communication. This method can ease key management especially for sensor nodes that have limited resource.

Two types of key predistribution schemes suited for WSNs have been developed: random key predistribution and deterministic key predistribution.

1) Random Key Predistribution:
According to this scheme, each sensor node receives a different random subset of keys from a large key pool as the node's key ring before deployment and then stores the key ring in its memory [3]-[5]. After sensor nodes have been deployed in the designated area, secure direct communication between two nodes requires that they share at least one common key.

2) Deterministic Key Predistribution: Combinatorial designs [6]-[9] are applied to key predistribution. They presented two classes of combinatorial designs. The combinatorial designs are associated with the distinct key identifiers and nodes, respectively. Though the probability of key establishment has been increased, this scheme is limited in network resiliency and network size.

B.HYBRID CRYPTOGRAPHY SCHEMES:
Though most framework use one type of cryptography, there still exist some schemes that use both asymmetric-key and symmetric-key cryptographs. For example, a hybrid scheme proposed by Huang[11], balances public key cryptography computations in the base station side and symmetric key cryptography computation in sensors side in order to obtain adorable system performance and facilitate key management. On one hand, they reduce the computation intensive elliptic curve scalar multiplication of a random point at the sensor side, and use symmetric key cryptographic operations instead On the other hand; it authenticates the two identities based on elliptic curve implicit certificates, solving the key distribution and storage problems, which are typical bottlenecks in pure symmetric-key based protocols.

C. ONE WAY HASH SCHEMES
To ease key management, many approaches use the one-way key method that comes from one-way hash function technique. For example, Zachary[12] propose a group security mechanism based on one-way accumulators that utilizes a pre-deployment process, quasicommutative property of one-way accumulators and broadcast communication to maintain the secrecy of the group membership. Another group security mechanism proposed by Dutta, also use one-way function to ease group node joining or revocation. Their scheme has self-healing feature, a good property that makes the qualified users recover lost session keys over a lossy mobile network on their own from the broadcast packets and some private information, without requesting additional transmission from the group manager. The one-way hash function can also adapt to conduct public key authentication. To ease the joining and revocation issues of membership in broadcast or group encryption, many approaches use predistribution and/or a local collaboration technique.

D.KEY INFECTION SCHEME
Contrary to most of key management using pre-loaded initial keys, Anderson[13], propose a key infection mechanism. In a key infection scheme, different from key pre-distribution schemes, no predistribution key is stored in sensor nodes. This type of schemes establishes secure link keys by broadcasting plaintext information first. This type of schemes is not secure essentially. However, Anderson, show that their key infection scheme is still secure enough for non- critical commodity sensor networks after identifying a more realistic attacker model that is applicable to these sensor networks. Their protocol is based on the assumption that the number of adversary devices in the network at the time of key establishment is very small.

E. KEY MANAGEMENT IN HIERARCHY NETWORKS:
In this type of key management, some use the physical hierarchical structure of networks, while others implement their hierarchy key management logically in physical flat structure sensor networks[14], which only include a base station and sensors. For example, LKHW (Logical Key Hierarchy for Wireless sensor networks), proposed by Pietro [16]-[18], integrates directed diffusion and LKH (Logical Key Hierarchy) where keys are logically distributed in a tree rooted at the key distribution center (KDC). A key distribution center maintains a key tree that will be used for group key updates and distribution, and every sensor only stores its keys on its key path, i.e. the path from the leaf node up to the root. In order to efficiently achieve confidential and authentication, they apply LKHW: directed diffusion sources are treated as multicast group members, whereas the sink is treated as the KDC.

IV.CONCLUSION
Thus, we provide features of various key management schemes for establishing secure communication in a

wireless sensor network .Security can be accomplished by adapting the type of Key Management based on the environment of WSN. In this paper, efficient cryptographic techniques have been proposed which ensures confidentiality, authenticity, availability and integrity of wireless sensor network that are deployed in hostile environment. Since key management plays a major role in encryption and authentication various schemes have been summarized by us. We have presented a nearly comprehensive survey of security researches in wireless sensor networks.

V.REFERENCES

[1]I.Akyildiz,W.Su,Y.Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114, Aug. 2002.

[2]A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security protocols for sensor networks," Wireless Netw., vol. 8, no. 5, pp. 521–534, 2002.

[3]L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proc. 9th ACM Conf. Comput. Commun. Secur., New York, USA, 2002, pp. 41–47.

[4]H. W. Chan, A. Perrig, and D. Song, "Key distribution techniques for sensor networks," in Wireless Sensor Networks. Norwell, MA: Kluwer, 2004,

[5]H. W. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proc. IEEE Symp. Res. Secur. Privacy, 2003, pp. 197–213.

[6]W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," ACM Trans. Inf. Syst. Secur., vol. 8, no. 2, pp. 228–258, 2005.

[7]R. Blom, "An optimal class of symmetric key generation systems," in Proc. EURORYPT 84 Workshop Adv. Cryptol.: Theory Appl. Cryptographic Tech., 1985, pp. 335–338.

[8]D. G. Liu, P. Ning, and R. F. Li, "Establishing pairwise keys in distributed sensor networks," ACM Trans. Inf. Syst. Secur., vol. 8, no. 1, pp. 41–77, 2005.

[9]S. A. Camtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor network," in Proc. Comput. Secur.- ESORICS, 2004, pp. 293–308.

[10]D. Chakrabarti, S. Maitra, and B. Roy, "A key predistribution scheme for wireless sensor networks:Merging blocks in combinatorial design," in Proc. Lect. Notes