Secured Communication in Wireless Sensor Networks

Jian Wang

\ *University of Teas at Arlington,*
Arlington, TX 77843

Email: {wang_jane@lycos.com}

Abstract

Recent advancement in wireless communications and electronics has enabled the development of low-cost sensor networks. The sensor networks can be used for various application areas (e.g., health, military, home). When the sensor networks are deployed in hostile environment, security becomes extremely important. To provide the security communication feature, the communication data needs to be encrypted and communication parties needs to be authenticated also. All these require effective security key management scheme. In this paper, we first study this special requirement for the sensor network and general key management problem; then we list some existing research work for the key management in the sensor network. Finally, we point out some open research issues and intend to spark new interests and developments in this field.

Keywords: *Wireless Sensor Network, Security, and Key Management*

I. Introduction

In this paper, we studied one of the fundamental security issues - secured key management in wireless sensor networks. First, we list and compare some existing research work in this area; then we point out the open research issues and intend to spark new interests and developments in this field.

Recent advances in microprocessor and wireless communication have enabled the widespread deployment of sensor networks consisting of small sensors with sensing, computation, and communication capability over a vast filed to obtain file-grained sensing data. There are many attractive applications for the sensor network such as, military target tracking, biology habitat monitoring, precise agriculture, environment control, etc. For example, environmental applications of sensor networks include tracking the movements of birds and insects, monitoring environmental conditions that affect crops and livestock, etc. According to sensor applications, the most fundamental task for the sensor network is data-centric information dissemination, in which applications can send queries to the sensor network and sensors measure the corresponding data for the queries and response to the applications.

From the security consideration, the wired network and wireless network are different. In the wired network, the adversary must gain physical access to wired link and sneak through security holes at the well-protected firewall before conducting attack. However, in the wireless network, the security becomes harder task due to following reasons:

1) There is no dedicated network infrastructure to conduct a clear line of defense,
2) Wireless attacker may come from all directions,
3) Every node must be prepared to encounter with an adversary.

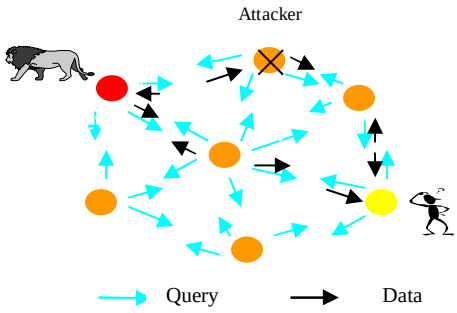

Figure 1: Sensor Network Query and Data Dissemination

Besides above property for the wireless network, there are following other limitations in the wireless sensor network:

1) Sensor nodes are limited in power, computational capacities, and memory,
2) Sensor nodes may not have global *identification* (ID) because of the large amount of overheads and large number of sensors. In this sense, the end-to-end secured communication such as, IPSec widely used in the Internet, is not a workable solution for the wireless sensor network. Figure 1 show an example, that application is interested in finding whether some animals are in certain regions by sending the query request to the

sensor network, but the application does not know which sensor satisfy its interest. After the query search process in the sensor network and the condition is satisfied (animal enter a certain region), the corresponding sensor node delivers the sensed data to the application through the sensor network.

As we mentioned above, the main task of sensor network to collect data for different applications and sensor network could be in a hostile environment, security becomes extremely important, as they are prone to different type malicious attacks. For example, an adversary can easily listen to the traffic, impersonate one of network nodes or intentionally provide misleading information to other nodes shown in the Figure 1. To provide the security, communication at both control plan and data plan must be enhanced by encryption and other security mechanisms such as, the communication parties must be authenticated before initiating communication, sensor query commands from the base station to the sensor node need to be encrypted hop-by-hop, and the run-time sensed data need to be encrypted hop-by-hop, etc. All these require effective security key management schemes.

The rest of paper is organized as follows: In Section II, we discuss necessary background about the security technology and sensor network. In Section III, we list and compare some existing research work on the security key management. In Section IV, we point out some open research issues and possible solutions.

II. Background

A. Sensor Network and Applications

A sensor network is composed of a large number of sensor nodes that are densely deployed either inside the phenomenon or very close to it. The position of sensor nodes need not be engineered or predetermined. This allows random deployment in inaccessible terrains or disaster relief operations. On the other hand, this also means that sensor network protocols and algorithms must possess self-organizing capabilities. Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are fitted with an onboard processor. Instead of sending the raw data to the nodes responsible for the fusion, they use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data.

Sensor networks may consist of many different types of sensors such as seismic, low sampling rate magnetic, thermal, visual, infrared, acoustic and radar, which are able to monitor a wide variety of ambient conditions such as, temperature, humidity, vehicular movement, lightning condition, pressure, soil makeup, noise levels, the presence or absence of certain kinds of objects, mechanical stress levels on attached objects, and the current characteristics such as speed, direction, and size of an object.

Sensor networks are being deployed for a wide variety of applications:

1) Military applications: Wireless sensor networks can be an integral part of military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting (C4ISRT) systems.

2) Environmental applications: Some environmental applications of sensor networks include tracking the movements of birds, small animals, and insects; monitoring environmental conditions that affect crops and livestock.

3) Health applications: Some of the health applications for sensor networks are providing interfaces for the disabled, integrated patient monitoring, diagnostics, drug administration in hospitals, monitoring the movements and internal processes of insects or other small animals.

4) Home automation: As technology advances, smart sensor nodes and actuators can be buried in appliances, such as vacuum cleaners, micro-wave ovens, refrigerators, and VCRs. These sensor nodes inside the domestic devices can interact with each other and with the external network via the Internet or Satellite. They allow end users to manage home devices locally and remotely more easily.

Sensor networks are different from traditional wireless networks: more constrained power, lower computation ability, smaller memory size, larger scale, different communication pattern, trust relationship among sensor network, security protocols for wireless networks are not suitable for sensor networks. With the scalable secured key management schemes, each sensor pair can setup a security key for the communication. Based on this, secured protocols for sensor application can be easily developed such as, the secured data routing/query and run-time data delivery with aggregation [3][4].

B. Security Technology

In network systems, there are many distributed resources, which can be used by applications. The security has become a major concern in network systems. Today, more and more systems are connected to the Internet. We enjoy the benefits provided by the Internet; however, we have to face many kinds of attacks on the infrastructure and systems connected to the Internet. Increasing attention has been given to the need for Information Assurance across critical information infrastructures. This need has been the focus of many groups and agencies like the National Security Agency, the National Telecommunications and Information Systems Security Committee to name a few. The Internet security problems are found everyday and have become the most important factor cumbering the development of Internet commercial application.

Generally, the security system should satisfy following several objectives: 1) Services can only be offered to authenticated users. 2) The users should have differentiated security requirements according to security policies. 3) The security system should have intelligent capability to monitor and audit security events, which makes the system more robust to prevent the attack. In order to satisfy these objectives, authentication, authorization and auditing (AAA) are required: 1) Authentication. Communication entities should have the capability to identify themselves to the communication party. 2) Authorization. Only the party qualifying access rules can use system resource. 3)

Auditing. This is the capability to record system security events, which helps the system to detect attack and response correspondently.

In these three AAA, the authentication is the first issue the security system must resolve. Currently, there are some authentication systems such as, Kerberos and Krypto-knight, which have been widely used in the field [1] [2]. In order to provide the authentication service, the communication parties need to have the security key. Due to this reason, the key management is a very important area for the authentication. In the distributed system, the secured communication is provided by the cryptogram mechanism. In the cryptogram research area, there are two types of cryptogram approaches: symmetric-key based and public-key based approach. For symmetric algorithms such as, DES and IDEA, a secure channel is required to setup the session key for the communication parties. Generally, the third part - authentication server as a trust coordinator has widely been adopted, which generates the conversation key and provides the secured channel. For the public key-based algorithm such as, RSA, communication party sends just needs to use other party's public key to encrypt the data and receiver uses its private key to conduct decryption. However, how to prove that public key is valid and truly associated to the corresponding party is also an issue. In order to handle this, an infrastructure-based public key distribution and validation mechanism are also needed and can also be generalized as the key distribution. In the following, we demonstrate the security key distribution protocol (Protocol 1) by following example shown in Figure 2.

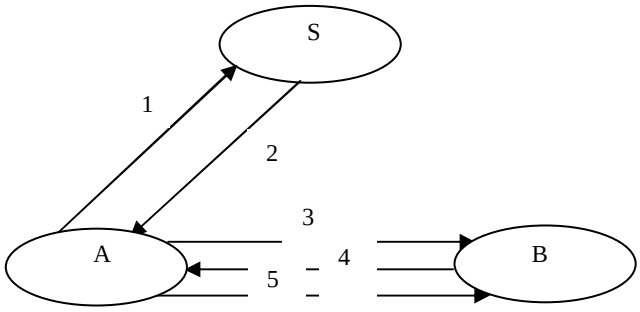

Figure 2: The Needham-Schroeder Authentication Protocol

Protocol 1:

A , B are authentication entities, which can be the user or process;
K_{as}, K_{bs} are privacy keys for authentication entities A and B, respectively;
S is the trusted third party to dispatch the session key for A and B;
K_{ab} is the conversational key dispatched by S;
N_a, N_b are nonce;

1. $A \rightarrow S : A, B, N_a$; A sends a request to S with source user id, destination user id, and a nonce.

2. $S \rightarrow A: \{N_a, B, K_{ab}, \{K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$; S dispatches a session key for A and B, which is encrypted by K_{as}.
3. $A \rightarrow B: \{K_{ab}, A\}_{K_{bs}}$; A sends the encrypted message to B, which includes the session key for A and B.
4 $B \rightarrow A: \{N_b\}_{k_{ab}}$; B receives the message from A and gets the session key from the message. To verify the identity of A, B sends a nonce encrypted by the session key.
5. $A \rightarrow B: \{N_b - 1\}_{K_{ab}}$; When receiving the nonce, A calculates a number using the pre-defined rule and sends it to B. Thus, A can prove its identity to B.

For the key management, there are three types of mechanisms for the key distribution: third party thrust server (shown in above example), self-enforcing, and key pre-distribution scheme. The *trusted-server* scheme depends on a trusted server for key agreement between nodes such as *Kerberos*. This type of scheme is not suitable for sensor networks because there is usually no trusted infrastructure in sensor networks besides the base station. The *self-enforcing* scheme depends on asymmetric cryptography, such as key agreement using public key certificates. However, limited computation and energy resources of sensor nodes often make it undesirable to use public key algorithms, such as *Diffie-Hellman* key agreement or *RSA*. The third type of key agreement scheme is key *pre-distribution*, where key information is distributed among network nodes prior to deployment. In general, the key pre-distribution scheme is more proper for the sensor network due to the sensor network limitation and we will discuss more about this in Section III.

III. Existing Key Management Schemes in Sensor Network

A. Overview

When the sensor network is deployed in a hostile environment, security is extremely important. An adversary can easily listen to the traffic, impersonate one of the network nodes, or intentionally provide misleading information to other nodes. The provide security, communication should encrypted and authenticated. To hide communication information among sensor nodes, the secret keys among communication nodes must be correctly set up.

Due to energy constraint, symmetric-key ciphers, low-energy, authenticated encryption modes, and hash functions become the mainly focus for secured sensor network communication. We can not directly adopt the traditional Internet style key exchange and key distribution protocols, which are based on infrastructures using trusted third parties, because of the unknown network topology before deployment, communication range limitations, intermittent sensor-node operation, and network dynamics.

The key distribution is the most fundamental issue in the sensor network. The most trivial solution is to generate a random key for each pair of users and transmits the key 'off-band' to the two parties through the security channel. This approach is unconditionally secure, but it requires a secure channel among each entity in the system and each entity must store n-1 keys and secured key distribution center needs to transmit total n(n-1) keys securely (this is sometimes called the n^2 problem) and each node needs to maintain n-1 security keys. Clearly, this approach is not scalable to the senor network due to its memory limitation. Some possible approach for the key pre-distribution is listed (detail descriptions are listed in the following section): 1) generate a large pool of P keys and of their key identifiers; 2) random drawing of k keys out of P keys without replacement to establish the key ring of a sensor; 3) loading of the key ring into the memory of each sensor; 4) saving of the key identifiers of a key ring and associated sensor identifier on a trusted controller node; 5) for each node, loading the i-th controller node with the key shared with that node.

Along with the pre-key distribution, there are two other types of key management schemes: share-key discovery and path key discovery schemes. The shared-key and path key discovery phase takes place during distributed sensor network initialization in the operational environment where every node discovers its neighbors in wireless communication range with which it shares keys. The simplest way for any two nodes to discover if they share a key is that each node broadcast, in clear text, the list of identifiers of the keys on their key ring. The shared-key discovery phase establishes the topology of the sensor array as seen by the routing layer of the distributed sensor network. A link exists between two nodes only if they share a key; and if a link exists between two nodes, all communication on that link is secured by link encryption. The path-key establishment phase assigns a 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 links at the end of the shared-key discovery phase. In the following section, we discuss some existing research work for the pre-key distribution, which is most fundamental problem in the sensor network and can easily support share-key discovery and path key discovery.

B. Existing Work for Key Management

For the key distribution in sensor network and considering the communication semantic, there are two main areas: one is for the key distribution for two pair communication parties just like the unicast-based communication scheme and the other is for the broadcast key distribution for group communication scheme.

1) Key management scheme for unicast-based authentication

Due to sensor network limitation, the most existing work is mainly focusing on pre-distribution-based approach. We list following several key pre-distribution schemes suited for sensor networks:

I) *Eschenauer and Gligor proposed a random key pre-distribution scheme as follows* [5]: before deployment, each sensor node receives a random subset of keys from a large key pool; to agree on a key for communication, two nodes find a common key (if any) within their subsets and use that key as their shared secret key. Now, the existence of a shared key between a particular pair of nodes is not certain but is instead guaranteed only with some probability (which can be tuned by adjusting the parameters of the scheme). The benefit of this approach is that the key distribution issue has been easily resolved. However, this approach cannot guarantee that each communication pair can always have the agreeable security key.

II) *Chen proposed an improved key management scheme based on deployment knowledge* [6]. The main idea of this work is to utilize "node deployment" knowledge, which might significantly improve the key pre-distribution problem. "Node deployment" information can be derived from the way that nodes are deployed. For example, when using airplane to deploy a sensor network, the sensor groups that are dropped next to each other have a better chance to be close to each other on the ground. The primary goal of secure communication in wireless sensor networks is to provide such communications among neighboring nodes. Therefore, the most important knowledge that can benefit a key pre-distribution scheme is the knowledge about the nodes that are likely to be the neighbors of each sensor node. Because of the randomness of deployment, it is unrealistic to know the exact set of neighbors of each node, but knowing the set of possible or likely neighbors for each node is much more realistic. Therefore, instead of guaranteeing that any two neighboring nodes can find a common secret key with 100% certainty, this paper also try to guarantee that any two neighboring nodes can find a common secret key with a certain probability P.

The advantage of this approach: key pre-distribution with deployment knowledge can substantially improve a network's connectivity (in terms of secure links) and resilience against node capture, and reduce the amount of memory required.

The disadvantage of this approach: to evaluate the performance of global connectivity, no theoretical analysis result, only simulation result is given. And this method is only the improvement of the original *Eschenauer-Gligor* scheme, it also assumes that sensors are static after being deployed without considering the dynamics of sensor network such as, senor node mobility, sensor node out of energy, etc. Also some open questions are not answered in the paper: will the small key set in the region makes adversary easier break down the system compared to large key set.

III) *Also based on Eschenauer and Gligor's scheme, Chan, Perrig and Song proposed a generalized "q-composite" scheme*. This scheme improves the resilience of the network and requires an attacker to compromise many more nodes in order to compromise any additional communications [7]. The major difference between this one and previous approach is that q-composite scheme is adopted and requires two nodes to find q (with q >1) keys in common before deriving a shared key and establishing a secure communication link. It is shown that by increasing the value of q, network resilience

against node capture is improved for certain ranges of other parameters. Clearly, this approach easily provides certain key redundancy and survivability capability under certain attack. However, the trade-off between efficiency and masking attack capability needs to conduct more investigation.

IV) *Du, Deng, Han and Varshney proposed a new key pre-distribution scheme [8]*. This scheme offers improved network resilience compared to the existing schemes Blom's key pre-distribution scheme by combining Blom's scheme with the random key pre-distribution method proposed by Eschenauer and Gligor. Blom's key pre-distribution scheme allows any pair of nodes to find a secret pairwise key between them, but it only requires nodes to store (λ+1) keys, where $\lambda << N$. But it sacrifices its some security properties. It has the following λ -secure property: as long as an adversary compromises at most lamda nodes, uncompromised nodes are perfectly secure. When an adversary compromises more than λ nodes, all pairwise keys in the entire network are compromised. Blom's scheme uses a single key space to ensure that any pair of nodes can compute a shared key.

In Du and Deng's paper they proposed a new scheme using multiple key spaces. First, construct a number of spaces using Blom's scheme and each sensor node carries key information from a randomly selected key space. So, if two nodes carry key information from a common space, they can compute a pair-wise key. Of course, it is no longer certain that two nodes can generate a pair-wise key (as in Blom's scheme); instead this improved method only has a probabilistic security key agreement guarantee. The analysis result shows that using same amount of memory (and the same probability of deriving a shared key, for the case of random pre-distribution schemes), the new scheme is substantially more resilient than Blom's scheme and the previous key pre-distribution schemes. Also a two-hop-neighbor key pre-distribution scheme is developed to further improve the resilience of our approach while maintaining connectivity of the network. The idea is to let the direct neighbor of sender forwarding messages, such that nodes that are two hops away are known as two-hop neighbors. Treating two-hop neighbors as "direct" neighbors as "direct" neighbors, the number of neighbors of each sender increases fourfold. The consequence is that the resilience threshold can be improved as well. The result shows that under certain conditions, the threshold can be improved a factor of four compared to the initial scheme.

2) Key management scheme for the broadcast-based authentication [9]

Like the unicast-based approach, broadcast authentication is also a fundamental security service in distributed sensor networks. Because of the large amount of sensor nodes and the broadcast nature of the communication in distributed sensor networks, it is usually desirable for the base stations to broadcast commands and data to the sensor nodes. In hostile environments, it is necessary to enable the sensor nodes to authenticate the broadcast messages received from the base station.

The original TESLA uses broadcast to distribute the initial parameters required for broadcast authentication. The authenticities of these parameters are guaranteed by digital signature generated by the sender. However, due to the low bandwidth of a sensor network and the low computational resources at each sensor node μTESLA cannot distribute these initial parameters using public key cryptography. Instead, the base station has to unicast the initial parameters to the sensor nodes individually, which severely limits the application of μTESLA in large sensor network.

μTESLA introduced asymmetry by delaying the disclosure of symmetric keys. A sender broadcasts a message with a Message Authentication Code (MAC) generated with a secret key K, which will be disclosed after a certain period of time. When a receiver receives this message, if it can ensure that the packet was sent before the key was disclosed, the receiver can buffer this packet and authenticate it when it receives the corresponding disclosed key. To authenticate the broadcast messages, a receiver first authenticates the disclosed keys. μTESLA uses a one-way key chain for this purpose,

IV. Open Research Issues and Solution

Most current existing work mainly considers the comparatively static sensor network. In other word, the sensor network topology is comparatively stable. However, the sensor node or communication entities can be mobile in the sensor network.

In this mobile sensor network without any fixed infrastructure, we can adopt the public key and symmetric-key integrated approach and design efficient key management system for the sensor network, which can allow each sensor node create, store, distribute, and revoke their public keys without the help of any trusted authority or fixed server. In the public-key structure, the authentication is performed via chains of public-key certificates in the following way: When a sensor node wants to obtain the public key of another sensor node, it acquires a chain of valid public-key certificates to validate the correctness of public key. Then the communication and authentication can be easily performed by the public key mechanism. As we mentioned, the public key to conduct the encryption can be very CPU consumption, the public and symmetric key combined key management can be a potential solution by following approach: the public key is used to conduct the authentication of communication parties and generate the session key for two sensor communication party, while run-time data encryption and decryption are performed by the symmetric-based session key.

Besides this, there are some new security research directions for the sensor network: as Distributed Deny of Service (DDoS) attack can initiate from different layers such as, physical, network, transport and application [10]. With the limited energy resource in the sensor network, designing the effective defense strategies in each protocol layers are also interesting issues and need more investigation.

References

[1] J. Steiner, C,Neuman, J.Schiller, “Kerberos: An Authentication Services for Open Network Systems”, *Proceedings of USENIX Conference*, 1988.
[2] R. Molva, G.Tsudik, K.V. Herreweghen, S.Zatti, “Krptoknight Authentication and Key Distribution Services”, *Proceedings of Esorics 92*, Oct., 1992.
[3] C. Kariof, D. Wagner, “Secure Routing in Wireless Sensor Networks: Attack and Countermeasures”, *Ad-hoc Journal*, 2003.
[4] A. Perrig, R. Szewczyk, V. Wen, D. Culler, “SPINS: security protocols for sensor networks”, *Proceedings of Mobile Networking and Computing*, 2001.
[5] L. Escheauer, V. D. Gliger, “A Key-Management Scheme for Distributed Sensor Networks”, *Proceedings of Computer Communication Security*, 1999.
[6] W. L. Du, J. Deng, “A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge”, *Proceedings of IEEE Infocom*, 2004.
[7] H. W. Chan, A. Perrig, D. Song, “Random Key Pre-distribution Schemes for Sensor Networks”, IEEE Symposium on Research in Security and Privacy, 2003.
[8] W. L. Du, J. Ding, “A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks”, *Proceedings of Computer Communication Security*, 2002.
[9] D. G. Liu, P. Ning, “Efficient Distribution of Key Chain Commitment for Broadcast Authentication in Distributed Sensor Networks”, *Proceedings of the 10th Annual Network and Distributed System Security Symposium*, pages 263-276, February 2003
[10] A. D. Wood, J. Stankovic, “Denial of Service in Sensor Networks”, *IEEE Computer*, 2002.