5.3 Key Management

Due to the characteristics of the wireless sensor networks, many popular and mature key management schemes in traditional wireless networks cannot be directly applied to wireless sensor networks. In the security solutions for wireless sensor networks, encryption technology is the basis for a number of security technologies, by encrypting wireless sensor networks that can meet the needs of certification, confidentiality, nonrepudiation, integrity, and so on. For encryption technology, key management is the key issue to be resolved.

5.3.1 Key Management Schemes Classification

In recent years, various key management schemes have been proposed. There can be a variety of categories for these schemes according to the characteristics of them. According to the cryptosystem they used, they can be divided into symmetric and asymmetric key management schemes. According to key distribution methods of the node, they can be split into random key management schemes and deterministic key management schemes. According to the network topology, they can be divided into distributed key management schemes and hierarchical key management scheme and various others scheme.

(1) **Symmetric and Asymmetric Key Management -** Depending on the difference of cryptosystem, the wireless sensor network key management can be divided into symmetric key management and asymmetric key management. In symmetric key management, the encryption and decryption key of the sensor node are the same, which is simple, and it has a small calculation and storage amount. Comparing with the asymmetric key, the symmetric key has an advantage in terms of computational complexity, but it is inadequate in the aspects of key management

and security. Asymmetric key management has been considered unsuitable for wireless sensor networks, mainly due to its relatively high requirement for computing, storage, and communication capabilities of nodes. But with the gradual deepening of the relevant studies, some asymmetric encryption algorithms can now be applied in wireless sensor networks.

(2) **Random and Deterministic Key Management -** According to the difference of the method in which nodes obtain the key, the key management in wireless sensor network can be split into random key management and deterministic key management. In the random key management, sensor nodes get their keys from the key pool or multiple keys space by random sampling. In deterministic key management, sensor nodes calculate the determination probability to get their keys. The advantages of random key management are a relatively simple way to get the key and the flexible deployment, and its disadvantage is that there may exist part of useless key information in the sensor nodes. The advantages of deterministic key management are that it can obtain more accurate key and the session key can be established directly between any two sensor nodes. Its disadvantage is that flexibility of deployment decreases and computational overhead of key negotiation becomes large.

(3) **Distributed and Hierarchical Key Management -** Depending on the topology of network, the wireless sensor network key management can be divided into distributed key management and hierarchical key management. In distributed key management, the computation and communication capabilities of sensor nodes are the same, and the key negotiation and update are completed through the mutual cooperation between sensor nodes. In hierarchical key management, network nodes

are split into clusters, and each cluster is composed of cluster head and ordinary sensor nodes. The ordinary sensor nodes complete key distribution, consultation, and update through their cluster head. The characteristic of distributed key management is that the neighbouring nodes collaborate to achieve key negotiation. The feature of hierarchical key management is that the requirement of computation and storage capacities of the common nodes is not too high, but once the cluster head is captured by the attacker, it will threaten the security of the entire network.

5.3.2 Typical Schemes of Key Management

1. Eschenauer and Gligor (E-G Scheme) first proposed a key management scheme for distributed sensor networks. The basic idea of the program is that a large key pool with the key and key identifier are generated first, each node could select different keys from the key pools randomly; such randomly pre-assigned manner made any two nodes have a certain probability of existing shared key. If there are shared keys between two adjacent nodes, then select one randomly as the paired key of the two sides to establish a secure channel. Otherwise, the entered node establishes a key path of the two sides through other neighbouring nodes that exists shared key after several jumps. The advantages of E-G scheme are mainly reducing the key storage pressure of each node and suitable for large- scale WSN key management. But there are also disadvantages of this program, and its security communication is uncertainly because the establishment of shared key is based on probability.
2. On the basis of E-G scheme, Chan et al. proposed a composite random key pre- distribution scheme. The specific implementation process of - composite random key pre-distribution scheme is basically similar to

E-G scheme, except that the E- G program just selects a public key as the main shared key between two nodes, while the -composite scheme requires that two adjacent nodes can establish the main shared key after the deployment only when there is at least shared key between them. Compared with the E-G scheme, the - composite program improves the capacity of resisting capture attacks of nodes but increases the overlap degree of shared key between the nodes and limits the scalability of the network.

3. Zhu et al. thought that any single key mechanism could not achieve the security needs of wireless sensor networks, so they proposed a LEAP protocol based on multiple key mechanisms to establish secure communications. The protocol maintained four keys in each node - a globally key shared with the base station, a group key shared with all nodes within the network, a paired key shared with neighbouring nodes, and a cluster head key shared with the cluster head. Compared with the random key pre-distribution protocol, the nodes' computation loads and storage space requirements for the LEAP protocol will increase, but it can guarantee that there is a shared key between the nodes needed to exchange data and support a variety of network communication modes.

4. Donggang et al. proposed a key distribution scheme based node group. The basic idea of the program is to assume the system to generate a large key pool beforehand, then it is divided into several subkey pools, making sure that each node deployment group has a corresponding subkey pool. Then the nodes of each deployment group select some keys from the corresponding subkey pool randomly. Due to the fact that the establishment of the secure channel between nodes needs at least one shared key, so it requires there should be public key between the

corresponding subkey pools of neighborhood groups to ensure the connectivity between nodes. Donggang et al. set up the repetition factor of the same key between the corresponding subkey pools of adjacent groups. The scheme is more safer, after the node is under attack, it has little impact on the security of other nodes in the network, but the storage overhead of such key management scheme is large; for the resource-constrained wireless sensor networks it is a very serious problem.

5. Du and Guizani et al. suggested that many key management schemes which based on symmetric key considered too much about network connectivity and hope to find a method that any two nodes can get shared key while ignore the communication of the two nodes. In the context of heterogeneous sensor networks, they proposed a route-drive public key management scheme based lightweight ECC, which only allocated communication key for neighbor node. The performance simulation shows that, compared to the symmetric key mechanism, this scheme significantly improved safety and also saved energy and storage space compared to key management schemes of other asymmetric key mechanisms.

5.3.3 Certification

Network security certification is another important part of the network. It includes identity authentication and message authentication, and methods used are symmetric encryption and asymmetric encryption method. This section summarizes research work on the two modes of certification.

5.3.3.1 Identity Authentication

Wireless sensor nodes are deployed to work after the domain, on the one hand, to ensure that users have the legal status to join the network, and, on

the other hand to effectively prevent unauthorized users from joining, so the wireless sensor network authentication mechanism must be used to determine the user's identity legitimacy. By using legitimate authentication of neighbouring nodes or nodes and base stations, wireless sensor network provides secure access mechanism, when all nodes access the self-organizing network. There are currently certified questions symmetric encryption algorithm based authentication methods and authentication methods based on asymmetric encryption algorithms.

(1) **Authentication Based Symmetric Encryption Algorithm -** In wireless sensor networks, due to the limited energy of nodes, the nodes of computing power and communication bandwidth, computational overhead of symmetric cryptosystem is much smaller than the asymmetric cryptosystem. Considered from the perspective of resource conservation, the symmetric cryptosystem is the most suitable characteristics for wireless sensor networks.

(2) **Authentication Based Asymmetric Encryption Algorithm -** Although symmetric cryptosystem has an advantage in the calculation of authentication, it has no strong asymmetric cryptography in terms of safety, and after the elliptic curve cryptosystem proposed, many studies show that even if there is a defect that the amount of computation and storage load are too large, asymmetric keys are still available for wireless sensor networks, asymmetric keys can still be used for wireless sensor networks. Here are some typical asymmetric cryptography schemes.

5.3.3.2 Message Authentication

Message authentication means to confirm the message received from sender statement. Message authentication can be achieved by symmetric encryption

and digital signature technology. At present, there are mainly two types of message authentication; one is point-to-point message authentication and the other is broadcast authentication. In a point-to-point message authentication, most of ID authentication methods can be to achieve. In wireless sensor networks, in order to save resources, broadcast is a common method of transmission. Currently, TESLA protocol is the most classic broadcast authentication protocol, and a lot of research work is commenced on the TESLA protocol.