Graduate Students: Ayishwarya Narasimhan, Vaishnavi Yekklur Balaji

Exploration of Key Management Strategies for Modern Internet of Things

Faculty Advisor: Dr. Wei Wang

Department of Computer Science, San Diego State University, USA

1. INTRODUCTION:

In this paper we present different key management schemes used in the wireless sensor networks delineating their similarities and differences and we also present a list of applications where it plays a major role. Internet of Things (IoTs) has attracted intensive interest from both academia and industry due to their wide application in civil and military scenarios. In hostile scenarios, it is very important to protect IoTs from malicious attacks. Securely designing wireless sensor networks is significantly challenging owing to its salient features and resource limitations. The security of a cryptographic system relies mainly on the secrecy of the key it uses. If an attacker is able to find the key, the entire system is broken because the attacker can use the key to decrypt the intercepted ciphertexts to find the original plaintexts. Hence numerous key management schemes have been proposed. The objective of key management is to dynamically establish and maintain secure channels among communicating nodes. The main features of key management in sensor networks include utilization of energy, localized impact of attacks, and scaling to a large number of nodes. The main challenge of key management is to manage the trade-off between acceptable security levels and conserving energy which is needed for network operations.

1. KEY MANAGEMENT PROCESS:

The key management has four basic functions. They are namely analysis, assignment, generation, and distribution of network keys. Key functions are triggered by keying events. The key events include network deployment, node addition, node eviction, or periodic key refresh. Entities with key management responsibilities may include a key server, base stations, and gateway nodes. The key analysis is the process of analyzing key requirements in order to determine the required number of keys for each nodes and number of keys for the entire network. The next step in the key management process is the key assignment. It refers to the mapping of keys to different parties. Key assignment may be static or dynamic depending upon the key management solutions employed. The administrative keys are generated once or multiple times over lifespan of the network. The generation of communication keys is the responsibility of the communicating parties such as sensor nodes, gateways, or base stations. The distribution of communication keys usually takes place after the network has been deployed. Communication keys are used for a short period of time and should be regularly updated.

* 1. TRADITIONAL KEY MANAGEMENT SCHEME:

The key management scheme has two major categories. They are namely traditional approach and dynamic approach. In the traditional approach, administrative key remains the same. It is also known as static key management scheme. A very important issue in sensor networks is how to securely manage the keys between the sender and the receiver. There are two types of keys are used in cryptographic systems. They are symmetric key and asymmetric key.

* + 1. SYMMETRIC KEY MANAGEMENT:

In a symmetric key system, the sender and receiver share a common key that is kept secret from others. The sender encrypts a plaintext *M* with the key *K* by an encryption algorithm *E* to get a ciphertext C. After receiving the ciphertext *C*, the receiver inputs *C* and the key *K* into a decryption algorithm *D* to get the original plaintext M. Symmetric key algorithms are those which require simple hash, rotation, or scrambling operations. These operations can be easily and efficiently implemented in hardware or software. Examples of symmetric key algorithms are Data Encryption Standard (DES) and Rivest Cipher 5 (RC5). Asymmetric key algorithms require exponential operations over a field modulo a large prime number are more complex than symmetric key operations. Examples of asymmetric key algorithms are Diffie-Hellman or Rivest Shamir Adleman (RSA). Therefore, the symmetric key technology is more suitable on resource constrained low-end devices than the asymmetric key technology. The main problem in using the symmetric key technology is to how to establish the symmetric key between two nodes. There are three major approaches to this main problem, namely Global, Centralized, and Pre-distribution approach.

* + 1. ASYMMETRIC KEY MANAGEMENT SCHEME:

In an asymmetric key system, each user has a pair of keys {*Ks*, *Kp*}. The user keeps secret his/her *private key*, *Ks*, while publishing his/her public key, *Kp*. Asymmetric key systems are called public key systems. Asymmetric key is computationally expensive but it is easier to manage and more resilient to node compromise than symmetric key technology. Each node can keep secret its private key and only publish its public key. Hence compromised nodes cannot provide clues to the private keys of non-compromised nodes.

The most challenging problem here is how to perform asymmetric key algorithms in an efficient way. One approach is to use specific parameters that can speed asymmetric key algorithms without compromising security. Tiny public key (TinyPK) uses RSA-based certificates to authenticate external parties before they can access the network, where the RSA public key is chosen as *e* = 3, such that the signature verification at the sensor side is simplified. Moreover, the Diffie-Hellman algorithm is used in TinyPK to exchange keys between sensor nodes, where the base of exponentiation is chosen as two, such that the exponential operation is simplified.

The second critical issue of applying asymmetric key technology is the authenticity of public keys. A public key should be owned by the node that claims to have it. Otherwise, attackers can easily impersonate any node by claiming its public key and launch the *man-in-the-middle* attack. Identity-based cryptography removes the necessity of public key certificates and thus saves cost on certificate authentication. Based on this technique, Zhang *et al.,* proposed the notion of *location-based* keys by binding private keys of individual nodes to their IDsand their locations. In this solution, the pairwise key of twoneighboring nodes is the by-product of their mutual authentication process. In addition, any two nodes that are a multihopapart can establish a shared key on demand, based on theirlocation-based keys. Their solution has perfect resilience tonode compromise in that no matter how many nodes are compromised,the location-based keys of non-compromised nodes,as well as their pairwise keys, always remain secure.

* 1. DYNAMIC KEY MANAGEMENT SCHEME:

A new emerging category of key management scheme called the Dynamic key management scheme. It changes administrative key periodically on demand or on detection of node capture. The main advantage of dynamic keying is enhanced network survivability, since any nodes major advantage of dynamic keying is enhanced network survivability, since any captured keys are replaced in a timely manner and the process is known as rekeying. Another advantage is support for network expansion, since upon adding new nodes the probability of node capture does not increase as the keys are rekeyed periodically unlike static keying which use fixed pool of keys. The major challenge in dynamic keying is to design a secure yet efficient rekeying mechanism. The one solution to efficient rekeying problem is using exclusion-based systems (EBSs); a combinatorial formulation of the group key management problem. The second solution is SHELL; it uses the EBS framework to perform rekeying within each cluster. Cluster gateways keep track of the key assignment but not the actual keys.

1. COMPARISON OF STATIC Vs DYNAMIC KEY MANAGEMENT SCHEMES:

The static and dynamic schemes share the idea of selecting a random subset of keys for each node out of a pool of keys. Static schemes tend to rely on using a larger key pool to enhance network resilience to attacks, whereas dynamic schemes use a limited pool of keys as well as a limited number of keys per node to achieve better network connectivity. However in the dynamic schemes resilience to attacks is primarily achieved by rekeying.

1. SECURITY ISSUES:

The two major security issues are authentication and secure routing.

* 1. AUTHENTICATION:

Authentication is very important because the wireless medium is open to unauthorized attackers who can modify packets. Therefore, every packet must be authenticated before the receiver submits it to higher layer applications. According to the communication pattern, authentication can be performed in one-hop unicast, multihop unicast, and broadcast.

* 1. SECURE ROUTING:

The goal of networking is to provide an infrastructure for delivering data from a source node to a destination node. Routing protocols are very important because they are responsible to find the path from source to destination and take charge of the delivery of data. In this way, the nodes in a network can collaborate with each other to fulfill various applications deployed in advance. If a routing protocol fails due to malicious attacks then the high level application also fails and hence network becomes useless. Hence secure routing is very critical to guarantee the network functionality in the face of malicious attacks.

* + 1. PROBLEMS

Karlof and Wagner pointed out that most routing protocols for WSNs are vulnerable to malicious attacks. Unencrypted packets that carry routing information are easily prone to attacks and the attacker may discover the entire network topology or may inject false routing information to launch a Sybil attack [27] or redirect packets to change network topology. Both of the attacks can change the network traffic pattern so that some malicious nodes can receive most of the traffic before it arrives at the Base Station. In data aggregation, the aggregation node can be compromised so that the aggregated data is tampered with. A non-aggregation node also can report false data to the aggregation node to disrupt the final report. A location deterministic operation is vulnerable because it requires cooperation among several nodes and may not be successful if some of them are malicious. A malicious node intentionally may drop some of the passing traffic. Of course, it can drop all the packets to act like a black hole, but this is easy to detect. Selective forwarding is more difficult to detect. A malicious node may drop the packets from some selected nodes and forward those from other nodes. A more subtle way is to drop packets intermittently so that it behaves like an unstable channel. Most routing protocols require that each sensor node periodically broadcast routing information to maintain the network topology. If the time synchronization in the maintenance operation is attacked, the whole network fails. Though several proposals tried to secure ad hoc routing protocols, they hardly can be applied in WSNs for two reasons. This is because all target ad hoc networks which are different to WSN and those proposals require either asymmetric key or complicated key cryptography which are quite expensive on sensor platform.

* + 1. AVAILABLE SOLUTIONS

Link-layer encryption and authentication by using a global key can protect WSNs against external attackers because they do not know the global key. However, this does not secure against node compromise because the global key can be exposed. A Secure Routing Protocol for Sensor Networks (SRPSN) is developed in [28]. A hierarchical network is constructed with cluster heads and cluster member nodes. Messages from sensor nodes are routed by cluster heads. To protect data, a preloaded symmetric key is shared between all cluster heads and the Base Station.

1. CONCLUSION:

Security has become a major concern for WSN protocol designers because of the wide security-critical applications of WSNs. Most security protocols are based on cryptographic operations which involve encryption keys.A secure management of these keys is one of the most critical elements in the WSN when integrating cryptographic functions into a system, since any security concept will be ineffective if the key management is weak**.**Key management in sensor networks raises interesting research issues. In this survey we presented different key management schemes and their applications. However, there are still many open issues and hence key management in WSN can be researched further in future.