A Study on Key Management Techniques in WSNs

MANUKRISHNAN P G
Dept. of Computer Science
GEC Thrissur

Prof. MANOJ KUMAR K V
Dept. of Computer Science
GEC Thrissur

Abstract— Wireless Sensor networks (WSNs) finds its applications in wide range of fields. They have been used extensively in critical infrastructures like battlefields, environment monitoring, fire detection, health applications etc... The WSNs consists of large number of sensors that are usually deployed from an airborne. Security is a major issue since they are usually deployed in hostile and unattended places. In order to achieve security in WSNs, it is required to encrypt messages sent among sensor nodes. In hierarchical sensor networks security can be achieved in different levels namely inter-cluster and intra-cluster. In this paper we perform a study on various techniques for implementing key management in WSNs mainly hierarchical sensor networks.

Keywords- Component; WSNs, Key management, Hierarchical WSNs.

I. INTRODUCTION

Recent advances in electronic and computer technologies have paved the way for the proliferation of wireless sensor networks (WSN). Sensor networks usually consist of a large number of ultra-small autonomous devices. Each device, called a sensor node, is battery powered and equipped with integrated sensors, data processing capabilities, and short-range radio communications. Sensor nodes are deployed either inside or very close to the sensed phenomenon. WSN is a network formed by large number of sensor nodes where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure etc... The need to monitor and measure different physical phenomena like temperature, fluid levels, humidity etc is common in many areas like structural engineering, agriculture and forestry, military sensing and monitoring. Wired networks were initially used but it becomes infeasible when the area to be sensed become hostile and difficult to monitor.

Sensor networks are being deployed for a wide variety of applications [1], including military sensing and tracking, environment monitoring, patient monitoring and tracking, smart environments, etc. When sensor networks are deployed in a hostile environment, security becomes extremely important, as they are prone to different types of malicious attacks [2].

II. NEED FOR KEY MANAGEMENT

The WSNs are usually deployed in hostile environments so security becomes a serious concern. Nodes deployed are susceptible to both internal and external attacks. Any adversary monitoring the sensor node can gain access to the critical information send between them or can inject bogus data. Such attacks are difficult to detect since the sensor nodes doesn’t communicate in a regular manner. They respond when the event to be monitored occurs. So the communication between the nodes must be protected using encryption techniques. For that encryption keys must be provided. Our paper focuses on the different schemes that exist for the management of keys.

Key Management is the management of cryptographic keys in the cryptosystem. It deals with the generation, exchange, storage, use and replacement of keys. Successful key management is critical to the security of a cryptosystems. The sensor nodes are limited in energy, bandwidth, processing power and memory. So the key management techniques must be energy efficient using less power and storage space. There are mainly two types of wireless sensor networks namely Flat network architecture and Hierarchical sensor networks. The key management techniques are different for them.

III. KEY MANAGEMENT TECHNIQUES

Eschenauer et al. [3] proposed a random key pre distribution scheme. Here a very large key pool is generated. And each sensor node is pre-distributed with a randomly selected set of keys. Then the sensors are randomly deployed. After deployment each node sends its key information to the neighbour. Since the keys are randomly selected from the same key pool some of the nodes will share some common key between them. If two nodes possess same key then they can communicate with each other. Otherwise a path-key establishment is performed that the sensors that don’t share keys could establish a path using intermediate nodes. But the intermediate sensors involved can degrade the network security and produces additional computational and communicational overhead. Various schemes that is based on the key pool were proposed.

Based on Blom’s method [4], Chien et al. [5] proposed a key pre-distribution scheme by using two $n \times n$ matrices: a public matrix $M$ and a secret symmetric random matrix $D$. The matrices $M$ and
sensor node stores only two keys—one it shares with allotted to them. Other time they are sleeping. The sensors will be in active mode only in the slot (TDMA) based Media Access Control where the network. This is a Time Division Multiple Access command node that controls the mission of the from different sensors and sends them to the event and the gateway node aggregates the data number of sensor nodes. The sensor nodes sense each cluster is composed of a gateway node and nodes partition the network into different clusters.

Cluster Communication is the one between member sensor nodes that belongs to the different levels namely Intra Cluster Communication and Inter Cluster Communication. Intra Cluster communication refers to the communication between the sensor member nodes that comes under the same cluster head (CH) whereas Inter Cluster Communication is the one between member sensor nodes that belongs to the different clusters.

In 2003, Jolly et al. [8] proposed a low-energy key management (LEKM) protocol for sensor-to-gateway keys management. In this model, the sensor nodes are deployed in the areas of interest. There are sensor nodes, command nodes and gateways. The gateways have comparatively high storage, energy and processing power. The gateway nodes partition the network into different clusters. Each cluster is composed of a gateway node and number of sensor nodes. The sensor nodes sense the event and the gateway node aggregates the data from different sensors and sends them to the command node that controls the mission of the network. This is a Time Division Multiple Access (TDMA) based Media Access Control where the sensors will be in active mode only in the slot allotted to them. Other time they are sleeping. The key management in this scheme is such that a sensor node stores only two keys—one it shares with the gateway and the other it shares with the command node. The command node has high storage and is situated in a friendly area. So it stores keys of all nodes. The gateway node stores keys it shares with the members in its cluster and the key it shares with the command node. Since the gateway node is preloaded with m/n keys in the initialization phase, the compromise of it can breach the security

V. INTRA-CLUSTER KEY MANAGEMENT IN HIERARCHICAL SENSOR NETWORKS

Liu Ya-nan et al. [9] proposed an intra-cluster key sharing technique for hierarchical sensor networks. This scheme has various steps that is discussed here.

Group deployment:- When the sensor nodes are deployed in the target field, there are many factors that will affect where a sensor node will finally be reside. When a sensor node is dropped from a helicopter, the final location where it is placed depends on the location and velocity of the copter when the nodes are dropped and the wind speed. However, since the sensor nodes in the same group will be deployed together, it is very likely that they are affected in a similar way by the same set of factors. Therefore, the final locations of the nodes in the same group will be close to each other with a high probability after deployment [10]. In this model the sensor deployment distribution is as a Gaussian distribution (also called Normal distribution). Gaussian distribution is widely studied and used in practice [2]. We call a group of sensor nodes that need to be deployed together as a deployment group. Each Deployment Group has a group header (GH).

Global Key Pool generation:- A global key pool is generated from which the keys are pre-distributed to each node without replacement.

Selection of virtual cluster heads:- For each node in the cluster randomly select d group headers (GH) as the virtual cluster heads. And these cluster heads will be designated with the share of a key for whom they are the virtual cluster head.

Creation of Shares:- The key is divided into different shares using Shamir’s Scheme. In 1979 George Blakley [11] and Adi Shamir [12] independently introduced a secret sharing scheme called a (k, n) threshold scheme. Their secret sharing scheme first divides the secret data into n pieces, with each piece called a shadow or a share. Then, the set of shadows is distributed to n participants, each of whom holds one shadow. Later, the secret data can be reconstructed if and only if there is at least complete knowledge of the k shadows, where k≤ n. There are two phases related
to creation of shares - Shares construction phase and Revealing phase.

Shares construction phase is done before deployment. The shares are created using Lagrange’s Interpolation and pre-distributed into the virtual cluster heads of each nodes.

Shamir’s scheme

In 1979, Shamir proposed a (k,n) threshold scheme based on a polynomial interpolation method [12]. In this scheme, the secret data s is divided into n pieces based on a polynomial sharing function of degree (k − 1) over an arbitrary finite field GF(q), where q is a prime number, by using

\[ f(x) = (a_0 + a_1x + \ldots + a_kx^k) \quad (1) \]

where \( a_0 = s \) and all other coefficients are random elements in the field. The share \( s_i = f(i) \) is given to the \( i \) th participant.

To reconstruct the secret data s from at least k shares arbitrarily chosen from n shares, we must first obtain the coefficients of the polynomial function \( f(x) \). These coefficients are obtained by using the Lagrange interpolation formula in

\[ \prod_{l=0,l \neq i}^{n} \frac{x-x_l}{x_i-x_l} \quad (2) \]

Then the polynomial function \( f(x) \) is determined as in

\[ f(x) = \sum_{i=0}^{k} (s_i x^i) \pmod{q} \quad (3) \]

Finally, the secret data s = f(0) is retrieved.

Initializing Phase:- The sensor nodes after deployment will form clusters using some clustering algorithms headed by the group heads (GH). Now they are called cluster heads (CH). If the cluster head and the group head are similar then called physical cluster head. If the group head and physical cluster head are equal then the key can be established directly otherwise indirect key establishment.

Direct Intra-Cluster key establishment: A member node S1 needs to communicate with another node S2 in the same cluster headed by CH1. Then S1 sends a request to CH1. CH1 broadcasts a “Share Request Message” to all cluster heads. The cluster heads who are virtual cluster heads of S2 will reply with their share. The private key is reconstructed in the cluster head CH1. This can be done so if the group head and the physical cluster head are the same. If not then the keys need to be established in the inter-cluster level.

VI. CONCLUSION

The intra cluster key sharing approach is discussed here. In [9] since only shares of the key are stored in the cluster heads, capture of a cluster head cannot compromise any key. Since a minimum number shares, k is required to reconstruct the key. So this scheme can be is highly reliable. Since most of the steps are done offline, it reduces the power consumed thus proves to be a good scheme for use in energy constrained sensor networks. The future work can be done that implements another technique for intra-cluster communication.

VII. REFERENCES


