A NOVEL KEY MANAGEMENT SCHEME FOR WIRELESS SENSOR NETWORKS

PRASHANT GAUTAM 1, NAVDEEP KAUR SALUJA 2.

1. M.TECH, SCHOLAR, DEPARTMENT OF COMPUTER SCIENCE ENGINEERING, INFINITY MANAGEMENT & ENGINEERING COLLEGE, SAGAR, (M.P.), INDIA
2. HOD, DEPARTMENT OF COMPUTER SCIENCE ENGINEERING, INFINITY MANAGEMENT & ENGINEERING COLLEGE, SAGAR, (M.P.), INDIA

ABSTRACT

The way that is used to achieve most important security requirements is the cryptography. Cryptography mainly depends on what is called cryptography keys; the cryptographic keys required to be managed by Key management plays a fundamental role in cryptography is to provide confidentiality, entity authentication, data origin authentication, data integrity, and digital signatures. The goal of a good cryptographic design is to reduce more complex problems to the proper management and safe-keeping of a small number of cryptographic keys, ultimately secured through trust in hardware or software by physical isolation or procedural controls. This paper presents a simple, efficient and secure scheme for key generation, distribution and storage for wireless sensor networks. The proposed algorithm is simulated using Matlab and compared with standard key management algorithm. The Proposed Algorithm shows that the delivery of rekeying messages reduces the communication of rekeying messages by about 5 times and storage space also reduced using Gaussian PDF.

KEYWORDS

Sensor network, Key management, Gaussian PDF, SEK & Key Establishment.
INTRODUCTION

Wireless Sensor Network (WSN) is the networks that consist of many small devices that called sensors. In literature, sometimes it is considered as a special type of the ad hoc networks [1]. These networks are useful in our life; they are widely used in many applications. WSN is used in military, commercial, and in ecological. Thus, the communications in these networks must be secure. Securing the communication in WSN is a very important issue, just because of many security threats and because of the nature of WSN [2]. By studying the communication links in these networks, which is the radio links that is subject to many faulty information and malicious attacks. Sensor devices in general have a limitation in its resources; these limitations can control the nature for WSNs, also affect the security level for this type of networks [3]. As an example for such limitations; limited processing power, battery age, transmission distance, shortage in memory space, random distribution for nodes, and bandwidth [4]. This paper represents the scheme of reducing key distribution time and storage requirement without compromising the security in WSN. The rest of the paper is organized as that second section presents a brief review of some of the recent work related to same field. The third section provides the overview of basic key management technique. The fourth section describes the proposed algorithm followed by the simulation results in fifth section and finally the conclusion on the basis of simulation results in section sixth.

LITERATURE REVIEW

Wireless sensor networks (WSN) are a type of wireless network that consists of distributed autonomous devices, referred to as nodes or motes, equipped with sensors to monitor environmental or physical conditions, such as humidity, temperature, pressure, sound, vibration, etc [5]. There are a wide variety of scenarios in which these networks can be used, such as environment and habitat monitoring, healthcare applications, security applications, home automation, tracking of military objectives and many more. In addition to the sensors, the nodes in sensor network are usually equipped with a radio transceiver, a small microcontroller and an energy source, which is typically a battery [6]. Since the WSN has such constraints, and is vulnerable to attackers, securing it is considered a great challenge. Many algorithms have been proposed in the literature to achieve this task [7]. WSN needs a cryptography algorithm that must be selected carefully, and the most important factor for those algorithms is solving the Key agreement or management problem, that is needed to provide an encrypted and authenticated data transmission between the sensors nodes to have a secure channel [8]. The cryptography algorithm has to meet many securities requirements such as, confidentiality, integrity, authenticity, and availability [9].
KEY MANAGEMENT SCHEMES

In this paper, we focus on the design of a multi-objective algorithm based on a tunable cost function to provide adaptability to existing routing protocols in order to meet several performance objectives. This function provides a general tunable model for supporting and meeting diverse application requirements, before and during network operation, by considering the changing conditions of the network as well as node resources. Rather than designing a new routing protocol, a solution that is flexible and easy to implement over several existing routing protocols. The proposed approach focuses on three main requirements although others can be considered:

1. **Network sustainability** – connectivity in the network must be maintained as long as possible
2. **Reliability** – a node’s level of busyness should be similar throughout the network to avoid losing packets routed through busy network areas.
3. **Delay** – packets should be delivered with minimum end-to-end delay

In this section, the ideas of distributing the key to the network topology are explained, and review the procedure to design topology aware key management schemes.

The most common method of multicast key management schemes uses a tree hierarchy for the maintenance of keys [2] [2_2] [2_4] [2_5].

![Figure 1: Simple topology of a network for key management tree.](image)

As shown in figure 1, the node A firstly generates a group (SK1, SK2,……..SKn) of session keys (SK) depending upon the number of users group required. These keys are used for multicasting. Now each SKi is need to be transferred securely to all the member of that group for that Mi (number of users in ith group) numbers of key encryption key (KEK) are generated which are used to encrypt the SK and send it to group members. It is clear that the each time the change in group users detected a new SK for all the users in that group is need to update this requires too much time also the large number of updated KEKs needed the storing of the KEKs is also required large memory.

**PROPOSED ALGORITHM**

The proposed scheme mainly focuses on the establishment and maintenance of the pair wise keys as well as the group keys. Unlike hierarchical and tree-based key management schemes, this scheme does not require additional memory for storing the keys after deployment. In this scheme, no key is broadcasted. Each and every node generates the group key and pair wise
key using one of the polynomial functions. The polynomial function is identified with the help of its ID. To enhance message security in the network initialization phase, each sensor node makes use of its own individual key. The base station computes the individual key of all the nodes using the unique keys and the IDs that it has stored. This method also enhances security in data transmission with periodic key update. To avoid the replay attack, sequence number is used. Therefore rather than complete keys we will solely send the rotations that rotate back the information to be sent. From the above discussion it is clear that for 32- bit key solely wont to at the start generate the 256 bits long keys at the nodes so once solely five bits needed to update it. The keys were generated by grasp configuration register the Group manager needn't to store all the keys instead solely the configuration and therefore the rotations keys were kept. There is no common key shared between the group of users each user has its own keys.

The proposed scheme has the following steps:

1. First Node initialization phase started in which sensor nodes become active to share data.

2. The root node calculates the number of nodes that establish the session for data sharing.

3. The Session keys are generated to the users or nodes that want to share data.

4. The Group Manager distributes the SEKs for all the users for data sharing.

5. If the change is detected a random range is generated by root node (as rotation number).

6. This range is transferred to any or all the users within the updated cluster.

7. Currently every user uses these rotation keys of update for their SEK.

8. If key found, then communication between nodes starts otherwise go to the step 2 and continues.
SIMULATION RESULTS

In the simulation setup, the number of users is 100. SEK length is 256 bits, KEK is also 256 bits, similarly SEK and KEK configurations are 32 bits respectively. SEK rotations are 16 bits for simulation time of 60 seconds. The network size is Gaussian pdf for mean 0 and variance as 1. Figure 3 shows the Network size Vs bits Over Head. Proposed Method the figure shows that maximum 3000 bits overhead. Figure 4 shows the Network size Vs bits Over Head. Standard Method the figure shows that maximum 8000 bits overhead. As network size increases proposed technique has 2.8% less Overhead. Figure 5 Network size Vs KEK overhead the graph shows that the proposed algorithm reduced the KEK overhead about 7 times.

Figure 3 shows the PDF for the network.

Network size Vs ESK overhead the graph shows that the proposed algorithm reduced the ESK overhead about 2 times as shown in Figure 4.

Figure shows that increase in number of user will increase the storage requirement of updated keys but has less in proposed scheme than as in previous scheme.
the storage overhead bits produced by Rotation Keys is shown in which proposed algorithm shows that the rotation keys also increases with the increase in the network size than previous scheme. Figure shows that increase in number of user will increase the storage requirement of updated rotation keys exponentially.

![User Keys storage vs No. of Users](image_url)

Network size Vs User Key Storage overhead the graph shows that the proposed algorithm reduced the SEK overhead about 8 times as shown in Figure 7.

CONCLUSIONS

The previous paper focused on a very significant security issue, which is the Key management in WSN. This problem has attracted the researcher's attention and makes them find out many techniques to solve it out. The Proposed key management scheme solved problem of security in WSN. This key management technique with less overhead by making use of pre-loaded information for security purposes in forming secure clusters and decrease some work efforts such as generating random number to get the number of needed iterations that would applied into uniform rule, and good robustness in facing WSN attacks. The proposed method also requires less storage space [12].

References


