

KEY MANAGEMENT FOR ENABLING SECURITY AGAINST INSIDER THREATS IN BODY AREA NETWORKS

¹C.G.Anupama, ²D.Anitha, ³Pooja Rajan

¹anupama.g@ktr.srmuniv.ac.in ²anitha.d@ktr.srmuniv.ac.in

³prajan199728@gmail.com

Abstract: Wireless Sensor Networks (WSNs) are a prominent fundamental technology of the Internet of Things (IoTs). Rather than device-to-device communications, group communications in the form of broadcasting and multicasting incur efficient message deliveries among resource-constrained sensor nodes in the IoT-enabled WSNs. Body Area Network (BAN) is an emerging field of WSN, where small wearable or implantable sensors are deployed inside and over the human body for health monitoring purpose. These networks require competitive protocol design to provide robust communication of health parameters for quick diagnosis and treatment. Due to the shared wireless medium between the sensors in BANs, it may be possible to have malicious attacks on e-healthcare systems. To achieve secure communications in such networks, sensor nodes (SNs) must establish secret shared keys with neighbouring nodes. Moreover, those keys must be free from the insider threats of corrupted nodes. This paper develops Location Dependent Key (LDK) management protocol for security against Insider Threats. Furthermore, the applicability of the protocol is analyzed and justified by an analysis of the security of the protocol proposed.

Index Terms: Body Area Networks, Insider Threats, Internet of Things, Location Dependent Key Management, Sensor Nodes, Wireless Sensor Networks.

1. Introduction

The Internet of Things (IoT) has become a powerful element of next generation networking technologies. In an IoT-enabled environment, things or physical objects no longer stay unresponsive. Instead they are connected to the Internet and embedded with processing and communication capabilities. Wireless Sensor Networks (WSNs) determine a key building block of IoT technologies. A WSN is a group of sensors used for collecting relevant data from the physical conditions of an environment and sending the collected data. A WSN

consists of hundreds to thousands of sensor nodes (SNs) performing wireless communication. Typically, sensors are considered resource-constrained devices with limited battery power and computation capabilities. WSNs not only measure environmental conditions such as temperature and sound but also gather sensitive data pertaining to people. Therefore, to prevent privacy issues, all communications should be carried out securely.

According to Gartner, the Internet of Things (IoT) will connect 26 billion devices by 2020 and will have a high economic value. WSNs are the foundation technique of the IoT, and for this reason, technical research in this area is being actively pursued. In particular, research applied to various fields such as military, medicine, industry, and traffic proceed continuously. For example, a patient data is collected and aggregated, and the required information is sent out to the relevant contacts (doctors or nurses). The aggregating unit collects data about the patient's ECG readings, blood pressure, etc. In turn, the processing unit determines the exact set of doctors, who should react according to the data acquired. Moreover, security is an important area in the study of WSNs because it uses actual data. Insider threats are a critical security issue in WSNs because standard security techniques like authentication and authorization cannot detect them. This is a serious threat for many applications such as military surveillance systems and other critical work fields.

The emergence in wearable sensors, resource-constrained circuits and wireless communication has enabled a new generation of wireless sensor networks, termed body area networks (BANs). BANs have the potential to collect, process, and send critical data for e-healthcare systems, which can provide new forms of hospitalization and quality health care. Wirelessly connected SNs placed in, on, and around the body form a BAN which allows continuous, automated, and remote monitoring of physiological signs to support medical applications. In addition, a patient controller (PC) is needed to perform multiple functions in BANs. A PC (such as a PDA (Personal Digital Assistant) or smart

phone) can sense and combine data from sensors all over the body, serve as a user interface, and bridge BANs to higher-level infrastructure.

Data confidentiality and integrity are the most important requirements in BANs, since the wireless medium is susceptible to a variety of security attacks. In this paper, we propose a location based key management as a core part of the research into BAN key management. Grid-based key management in location based key management helps in placing an SN in an assigned grid. Our main motto is to produce a key management that can withstand security attacks from malicious insiders such as off-duty doctors or discharged patients, and also that a hospital can make sure that SNs are correctly and securely associated with the intended patient.

The rest of this paper is structured as follows. We look at preliminary steps in Section II. We describe our protocol in Section III. Security analysis is described in Section IV. In Section V, we look at related work, and finally, we present our conclusion in Section VI.

2. Preliminaries

In this section, we offer background knowledge before presenting our scheme. We describe the protocol model and threat model briefly. Notations used in our protocol are showed in Table 1.

A. Protocol Model

We propose a BAN model that is composed of a Hospital Device (HD), a Patient Controller (PC), Anchor Nodes (ANs), and Sensor Nodes (SNs). The SN gathers data from around itself and sends the data to the PC through hop-by-hop. The PC collects the data received from SNs and transmits to the HD. An AN transmits different cryptographic nonces to SNs according to a power level. The SN generates a pair-wise key using these nonces received from the AN. Fig.1 shows the protocol model that we are assuming.

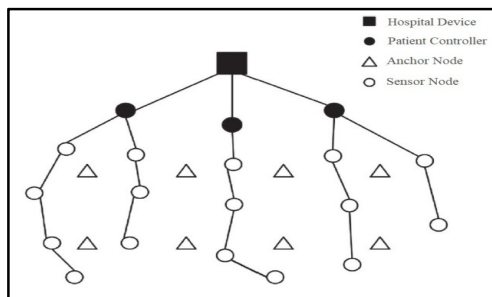


Figure 1. The Protocol Model

B. Threat Model

In this paper, we consider a variety of insider attacks. An insider attack is critical because it dodges authentication and authorization and drops important packets. Various types of insider attacks include modifying, misrouting, eavesdropping, and packet dropping. The packet drop attack is difficult to detect. Packet drop attacks also decrease network performance. Packet drop attacks comprises of blackhole attack, grayhole attack, or on-off attack. Because of the characteristics of grayhole and on-off attacks, they are more difficult to detect than blackhole attacks.

C. Notations

Table 1 shows the symbols and their description used in this paper. It is used to describe methods and results of the protocol.

Table 1. Notation.

Symbol	Description
HD	Hospital Device
PC	Patient Controller
AN	An anchor node
AN_{set}	A set of anchor nodes
SN	A sensor node
SN_{set}	A set of sensor node
k_c	A pre-distributed network key
G	A pre-distributed nine-grid information
H	A pre-distributed hash function
N_r	A transmitted cryptographic nonce
K_t	A key generated using nonce and grid
K_s	A communication key

3. Protocol Solution

This section describes the proposed key establishment process using ANs based on LDK. LDK has two steps. First, SNs generate a communication key to manage keys. Second, the keys are updated to secure the network against insider threats. Each SN stores a network key, a hash function, and the additional grid information, which is pre-distributed to a HD. The total number of grid data is 9, and these data consist of the coordinates of the grid containing the SN and eight neighbour grids. After the SN is deployed in a field, the AN sends cryptographic nonces at different power levels. The Fig.2 below is an illustration of the above described process.

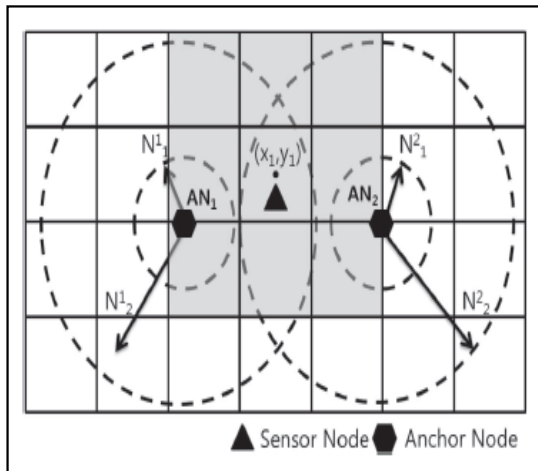


Figure 2. Illustration of grid system and LDK

A. Key Generation

To secure against various active attacks, there are four steps to establish a communication key in LDK, i.e., the pre-distribution phase, the initialization phase, the key establishment phase, and the key agreement phase, which are explained in detail in the following sections.

1. Pre-distribution Phase:

In the pre-distribution phase, SNs save the information that is needed to manage the key before a deployment. The factors saved in SNs are described as follows:

- a network key, k_c for secure communication,
- a communication key K_s ,
- a hash function H that is used to generate a key,
- the nine-grid information G_i ($1 \leq i \leq 9$).

The process of initiating blackhole attacks can be divided into three sequential stages. First, the attacker captures an SN and extracts critical information. Second, the attacker redeploys a corrupted SN to BANs. Finally, the actual blackhole attacks are launched. Hence, before the key is generated, we consider preventing node capture as a potential countermeasure against blackhole attacks. Each SN generates its neighbour table using a hello message. An SN recognizes the nodes that send an acknowledge (ACK) message as neighbour nodes. The following algorithm shows the method of creating a neighbour table:

```

SN0 → SN1 : hello message
IF SN1 → SN0 : ACK
    SN0 : add SN1 to Neighbour set
ELSE
    SN0 → SN1 : hello message

```

hello count of SN₀ = hello count of SN₀+1.

2. Initialization Phase:

The initialization phase is a process by which an SN is transmitted from ANs. In this phase, the cryptographic nonce revision is progressed. The AN transmits encrypted nonces to SNs at different power levels. After receiving nonces from ANs, the SN transmits the encrypted coordinates of its assigned grid to the neighbour nodes. The neighbour node, which has the same coordinates in the grid mapping as the assigned grid, transmits the number of nonces to the SN. If the number of nonces transmitted by the other neighbour node is greater than its own number of nonces, the SN requests the nonces from that neighbour node to revise its own nonces.

3. Key Establishment Phase:

In the key establishment phase, a SN generates a key by combining nonces and the nine-grid information, and by using the hash function with a network key. The following algorithm shows the key establishment phase for SNs:

$$SN_{set} : K_t = H_{k_c}(N_r \| G(x, y)).$$

4. Key Agreement Phase:

In the key agreement phase, the SNs generate a communication key with its neighbour nodes. The SNs encrypt all the keys that it generated and attaches a MAC value to ensure integrity. The neighbour node checks whether it has the same keys among its transmitted keys. If the number of the same keys is higher, the SN generates the communication key by implementing an EXCLUSIVE-OR (XOR) operation with the same keys.

B. Key Updating

An encrypted communication is of no use if an insider threat occurs while the network is working. In this section, we explain the node addition process, rekeying, and the revocation process with the help of which the key is re-established, to recover the network when a packet drop attack occurs.

[1]Node Addition:

An add node is deployed after it is registered. A HD transmits an authentication value of the nodeID added to the PC. After sending a hello message to its neighbour nodes, the neighbour nodes require authentication from the PC. The authenticated nodes request nonce from neighbour nodes through the initialization phase and

generate a communication key with neighbour nodes through the key establishment phase.

[2]Rekeying and Revocation:

Each SN collects data for its own purpose and transmits to a HD. Because the data transmitted to a HD are composed of a PC, this paper only considers the hop-by-hop data transmission from an SN to a PC. After all the steps of key generation are performed, a routing path would be determined by a routing protocol. The main point of key is that an SN does not need to share a communication key with all of its neighbour nodes. Therefore, the communication key is only maintained with maximum chosen neighbour nodes for the path determined by the routing protocol and the rest are deleted. The considered path is from an SN to the neighbour nodes. The neighbour node to which the SN first sends data is determined by the descending order of the routing path. This means that the data are transmitted in the form of a tree-form routing path.

In this protocol, each SN performs two processes to resist an insider threat. An SN maintains a sequential transmitted data from other SNs when the SNs transmit data in a hop-by-hop form. When authenticating the transmitted data, a sequence number renewal process of the source node data is performed. If the difference between the transmitted sequence number and the previous sequence number is larger than the threshold value, the node that transmitted the data is deleted from the neighbour table. Afterward, a rekeying command packet is delivered to a HD to notify it that a key renewal process of the whole network is needed. Algorithm 1 shows the rekeying process. The HD transmits a rekeying message to all the ANs, and the ANs transmit new nonces to the SNs. After that, a new communication key is generated.

Algorithm A1: Rekeying Alarm

```
Each received packet
If  $\tau > \text{sequence number}_{\text{curr}} - \text{sequence}$ 
    numberprev
    remove the node
    alarm the HD
Else
    processing packet
```

The SN that sends the data uses a hash function to generate the MAC of a sequence number. The SN that receives the data authenticates a transmitted sequence number to check if it has been modified by an attacker through MAC authentication.

Each SN computes costs according to each cycle and decides the next neighbour node that will send the data.

First-in-first-out (FIFO) is used to compute costs such that the most recently linked neighbour node gets the lowest priority. The cycle that changes the neighbour node is differently computed according to each SN. When the SN changes its neighbour node, it sends a hello message to the neighbour node to check if it is active. If the neighbour node does not return an ACK message, the SN deletes the information of the neighbour node and repeats the same process with the next neighbour node. Algorithm 2 shows the process for changing the neighbour node.

Algorithm 2: Changing the Neighbour Node

FIFO (a list of neighbour nodes)

At certain interval

If next neighbour node == active

change the next hop

Else

remove the next neighbour node

find the next hop.

4. Security Analysis

We give examples of some typical insider attacks on BANs and demonstrate how our protocol can prevent them. We also focus on certain circumstances in which packet drop attacks occur.

A. Blackhole Attack

In the protocol, SNs periodically change neighbour nodes according to a cost value. A blackhole attack is when a node drops all of its packets. When the attack occurs, each SN periodically changes neighbour nodes using cycle information and a cost value. If the next node drops all the packets, it cannot send an ACK message in response to the corresponding hello message. With the protocol, the node will check the next node. When a blackhole attack occurs, our scheme proposes a method of self-organization to minimize the damage in the BAN key management.

B. Grayhole and On-Off Packet Drop Attacks

The protocol is resistant to grayhole attacks and on-off packet drop attacks. A user can prevent such attacks by changing neighbour nodes periodically. However, because the packets are dropped randomly, the possibility that a corrupted node could still pass an active test exists. Therefore, the protocol mostly resists grayhole and on-off packet drop attacks. The attacks can be blocked using a rekeying method with the sequence number. When packets are dropped, there is a difference in

sequence numbers. Because SNs manage the sequence number of neighbour nodes in the form of a table, they can recognize the attack by comparing the sequence number when they receive the transmitted data after the packet drop. When the attack occurs, they request a key update from a HD. The corrupted nodes are excluded during the key renewal. Therefore, BANs can be secured against these attacks by using the sequence number method.

5. Related Work

In BANs, key management is a non-trivial issue, because a hospital must check whether a group of sensors are correctly and securely associated with the intended patient before any data communication happens. A lot of previous work focused only on key pre-distribution in sensor nodes.

Eschenauer and Gligor extracted a certain size of key rings from a large key pool in a server, and they distribute key rings before SNs are deployed. The deployed SNs use a commonly stored key in the key rings of two nodes to generate a pair-wise key for secure communication with the neighbour nodes.

Many recent BAN key management studies proposed a hierarchical architecture for networks, which are composed of a HD, a PC, and SNs. This is because SNs make it hard to apply a high computational cryptographic method due to inadequate hardware performance. Instead, they applied cryptographic methods to PCs that have greater hardware performance than an SN. Moreover, to resist various types of insider attacks, researchers applied a time stamp to authenticate packets and provided key revocation through the periodic authentication of SNs.

Location-based key management for WSNs usually use grid information. The grid information includes the coordinate after an area is divided into grids.

In 2006, Anjum proposed a scheme called LDK that generates a key by combining a pre-distributed key ring with cryptographic nonces. In 2010, Anjum extended the scheme. In contrast to schemes that are dependent on the position of grids, LDK is dependent on the position of SNs. Using a feature of the AN that transmits data within a certain distance by adjusting its power level, an area is divided. An SN is distributed to an area after storing a single common key K and hash function H . ANs transmit cryptographic nonces at different power levels, and a SN generates single key. When an SN finds common keys whose number is larger than the number of keys with a neighbour node, a communication key is generated.

6. Conclusion

The BAN system provides a flexible, wearable infrastructure for collecting, processing and wirelessly transmitting the medical data and information about the human body. Using BAN, multiple vital signs can be wirelessly monitored even in changing environments.

In this paper, we have presented an improved version of the LDK. We added rekeying technique by incorporating the use of grid information, and we suggest key generation by combining the grid information. Thus, we solve the problem of insufficient numbers of cryptographic nonces that can occur under the condition of communication interference. We also consider key generation and key revocation, as well as blackhole, grayhole and packet drop attack among the insider attacks. Through this protocol, we confirm that it provides higher connectivity and a lower compromise ratio, which means that stability and security are improved.

References

- [1] SH Seo, J. Won, S. Sultana, and E. Bertino, "Effective Key Management in Dynamic Wireless Sensor Networks", Feb 2015.
- [2] J. Shen, H. Tan, S. Moh, I. Chung, Q. Liu, and X. Sun, "Enhanced Secure Sensor Association and Key Management in Wireless Body Area Networks", Oct 2015.
- [3] F. Gandino, R. Ferrero, B. Montrucchio, and M. Rebaudengo, "Fast Hierarchical Key Management Scheme With Transitory Master Key for Wireless Sensor Networks", Dec 2016.
- [4] P. Porambage, A. Braeken, C. Schmitt, A. Gurtov, M. Ylianttila, and B. Stiller, "Group Key Establishment for Enabling Secure Multicast Communication in Wireless Sensor Networks Deployed for IoT Applications", Aug 2015.
- [5] F. Gandino, B. Montrucchio, and M. Rebaudengo, "Key Management for Static Wireless Sensor Networks With Node Adding", May 2014.
- [6] J. Choi, J. Bang, LH Kim, M. Ahn, and T. Kwon, "Location-Based Key Management Strong Against Insider Threats in Wireless Sensor Networks", Jun 2017.
- [7] M. Patel, and J. Wang, "Applications, challenges, and prospective in emerging body area networking technologies", Feb 2010.

- [8] K. Lorincz, D.J. Malan, T.R.F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton, "Sensor networks for emergency response: Challenges and opportunities", Oct-Dec 2004.
- [9] W. Jia, H. Zhu, Z. Cao, X. Dong, and C. Xiao, "Human-factor-aware privacy-preserving aggregation in smart grid", Jun 2014.
- [10] T. Kwon, and J. Hong, "Secure and efficient broadcast authentication in wireless sensor networks", Aug 2010.
- [11] P. Gaj, J. Jasperneite, and M. Felser, "Computer communication within industrial distributed environments-Survey", Feb 2013.
- [12] M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks", Feb 2013.
- [13] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks", May 2003.
- [14] W. Du, J. Deng, Y.S. Han, and P.K. Varshney, "A key predistribution scheme for sensor networks using deployment knowledge", Jan-Mar 2006.
- [15] X. Hu, L. Yang, and W. Xiong, "A novel wireless sensor network frame for urban transportation", Dec 2015.
- [16] E. Onur, C. Ersoy, H. Delic, and L. Akarun, "Surveillance with wireless sensor networks in obstruction: Breach paths as watershed contours", Feb 2010.
- [17] S. Keoh, S. Kumar, O. Garcia-Morchon, E. Dijk, and A. Rahman, "DTLS-Based Multicast Security for Low-Power and Lossy Networks (LLNs)", Feb 2014.
- [18] J. Zhang, and V. Varadharajan, "Wireless sensor network key management survey and taxonomy", March 2010.
- [19] Harikishore Kakarla, Madhavi Latha M and Habibulla Khan, "Transition Optimization in Fault Free Memory Application Using Bus-Align Mode", European Journal of Scientific Research, Vol.112, No.2, pp.237-245, ISSN: 1450-216x/135/1450-202x, October 2013.
- [20] Rajesh, M., and J. M. Gnanasekar. & quot; GCCover Heterogeneous Wireless Ad hoc Networks.& quot; Journal of Chemical and Pharmaceutical Sciences (2015): 195-200.
- [21] S.V.Manikanthan and V.Rama "Optimal Performance Of Key Predistribution Protocol In Wireless Sensor Networks" International Innovative Research Journal of Engineering and Technology, ISSN NO: 2456-1983, Vol-2, Issue –Special –March 2017.
- [22] T. Padmapriya and V. Saminadan, "Distributed Load Balancing for Multiuser Multi-class Traffic in MIMO LTE-Advanced Networks", Research Journal of Applied Sciences, Engineering and Technology (RJASET) - Maxwell Scientific Organization, ISSN: 2040-7459; e-ISSN: 2040-7467, vol.12, no.8, pp: 813-822, April 2016.

