RESEARCH ARTICLE OPEN ACCESS

ZigBee Security for Home Automation: A Comparison of Different Approaches

Jisna V A [1], Sobha Xavier [2],Ninu Francis [3]
Assistant Professor
Department of Computer Science and Engineering
Jyothi Engineering College
Cheruthuruthy - India

ABSTRACT
ZigBee is a specification defining a set of protocols and architecture for monitoring and controlling networks. With the advantages of high availability, low cost and low power consumption, ZigBee is ideal for both residential and industrial settings. There are different approaches for security in ZigBee networks. The approaches include Current ZigBee security, Public Key Cryptography, Identity Based Cryptography, Attribute Based Cryptography and Attribute Based Proxy-Re-Encryption. The paper makes a comparison on different approaches for ZigBee security. The paper also attempts to find which of the approach enhances the security features in ZigBee networks while reducing the number of required keys.

Keywords:- ZigBee, AES

I. INTRODUCTION

All kind of portable applications tend to be able to communicate without the use of any wires. Aim of a wireless communication is to gather information or perform certain task in the environment. With the rapid development of the wireless network technologies, the Home Automation (HA) system based on the wireless sensors networks (WSN) becomes more and more practicable. The technology provides new opportunities such as increasing the availability of home appliances and monitoring the electric meters.

To utilize the home automation, devices are connected between each other and communicate messages. Among all the Wireless Sensor Network (WSN) technologies, such as Bluetooth, ZigBee, UWB, Wi-Fi and NFC, the ZigBee technology is the most suitable one in the HA system design. The ZigBee technology is designed for the systems consisting of unsupervised groups of devices in houses, factories and offices. Zigbee is one of the most widely utilized Wireless Sensor Network standards with low power, low data rate, low cost and short time delay characteristics, simple to develop and deploy and provides robust security and high data reliability. The word Zigbee comes from zigzagging patterns of honey bees between flowers, that represents the communication between nodes in a mesh network [1].

However, current ZigBee network is not an attractive technology for security in terms of key management and capability of services. ZigBee occupies huge spaces to store a lot of keys and does not offer the capability of decryption.

With the advantages of high availability, low cost and low power consumption, ZigBee is ideal for both residential and industrial settings. But, security features in ZigBee networks which required a number of keys, consisting of master keys, network keys, link keys and don't offer various services depended on users. The paper focuses on different approaches for security in ZigBee networks.

This paper is organized as follows: Section II makes a literature survey on recent approaches towards ZigBee security for home automation. Section III makes a performance comparison on different approaches. Section IV discusses the scope, future works and concludes the work presented here.

II. RELATED WORKS

The recent approaches in ZigBee security for home automation include Current ZigBee security approach, Identity based encryption, Attribute based encryption, and Attribute based proxy re-encryption. Following sections will give a brief idea about the approaches.

2.1 Current ZigBee Security

ZigBee utilizes a symmetric cryptography scheme with 128-bit AES algorithm, a strong and secure encryption method approved by National Institute for Standards and Technology and provide data transmission confidentiality, replay attack and integrity [2]. There are three key types in ZigBee- master key, link key and a network key. Even though ZigBee offers strong method to protect information to attacker, ZigBee has restriction which involves a large number of keys and network key is inefficient. The second, network key is restricted in providing various services. As it is based on

symmetric key cryptography, this model doesn't provide digital signature [2].

2.2 Identity Based Encryption (IBE)

Identity based cryptography [2] is based on public key cryptography, using public and private key pairs to encrypt and decrypt information. In an identity based encryption, when owner of home enters a room, Zigbee device of door sends message which is encrypted using identity of trust center to trust center. Each message encrypted each devices identity. The working principle of identity-based cryptography is similar to that of public key cryptography.

When using identity-based cryptography for security in ZigBee, each network device uses some information to identify and distinguish itself from other devices. The device will use that identification as its public key for secure information exchange with other devices.

Fig. 2.1 shows an example home automation in which identity based cryptography is applied [2]. When owner of home enters the room 2, Zigbee device of door sends message which is encrypted using identity of trust center to trust center. After receiving the message, trust center sends message to air conditioner 2 and light 2 and they turns on. Each message encrypted each devices identity.

In spite of the advantages, identity based encryption has some problems [1]. If the private key is compromised, there is a problem of whether the owner needs to change his identity information corresponding to that private key. This requirement seems to be impractical if the identity information is owners representation in real life(name, office numbers or email addresses).

Even though identity based cryptography has both strong and weak points, it can be applied in some environments, e.g. a closed group where public key generator is trusted [2].

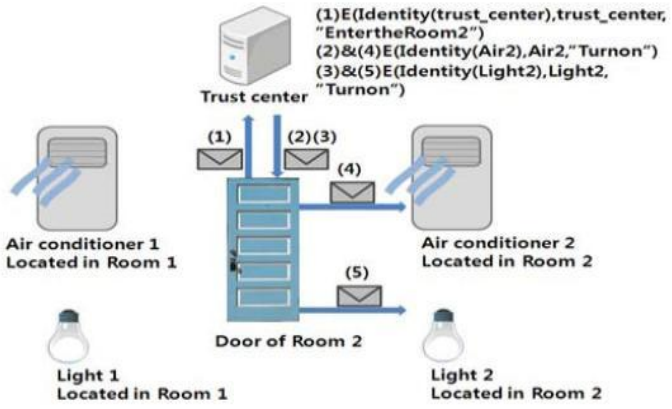

Figure 2.1: Home Automation using Identity-based encryption

2.3 Attribute Based Encryption (ABE)

Attribute-based encryption [3] is simpler then IBE and encrypts the message using attributes that provides various securities in ZigBee. An IBE, needs two time transmissions or more to send message to each node, but ABE sends once as a broadcast message. If nodes have attributes of room 2, nodes decrypt the messages. Therefore, we can send message to destination more efficiently. And, network is not centralized to trust center, because sender can encrypt the using attributes that does not need to negotiation from trust center. Trust center is used once in initialization phase.

2.3.1 Procedure of attribute-based encryption

The encryption/decryption working principle is described in fig. 2.2 [3]. In the rest of scheme, Public Key Generator (PKG) generates Master-key and Public-key from security parameter. Master-key is used to generate nodes Private keys and Public-key is used to encrypt and decrypt the message. After generating the Public-key, PKG distributes Public key to each node. When sender decided to send a message to node(s) that has specific attributes, sender encrypts the plaintext to the ciphertext using the access structure which represents attributes. When recipient received the ciphertext, recipient decrypts the ciphertext using attributes. If recipient satisfied the access structure of ciphertext, it will be decrypted.

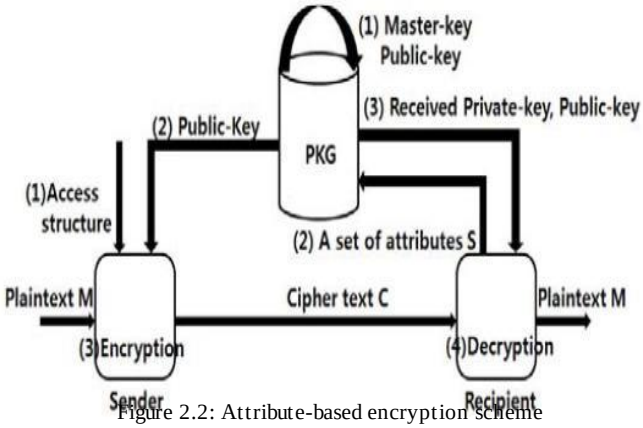

Figure 2.2: Attribute-based encryption scheme

2.3.2 Home automation using attribute-based encryption

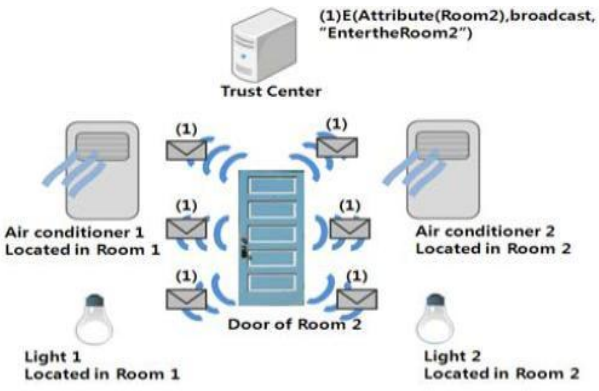

Figure 2.3: Home Automation using Attribute-based encryption

Fig. 2.3[3] shows an example home automation in which attribute based cryptography is applied. When the owner enters the door of room 2, a message is broadcast. If the devices receiving the message have the attribute of room 2, the device decrypt the message and performs the required action. In fig 2.3 air-conditioner 2 and light 2 decrypt the message and they turns on.

2.4 Attribute-based Proxy Re-Encryption(ABPRE)

Proxy re-encryption (PRE) allows a proxy server to re-encrypt a ciphertext with other attributes. Users delegate part of his decryption capability to others. The user designates a proxy server which can re-encrypt a ciphertext related with a certain access policy.

2.4.1 Procedure of attribute-based proxy re-encryption

The encryption, re-encryption and decryption working principle are described in fig. 2.4 [4]. Firstly the basic scheme of attribute based encryption is presented. First, PKG generates a master-key and public-key from security parameter. The master-key is used to generate nodes private keys and a public-key is used to en-crypt and decrypt the message. After generating the public-key, PKG distributes the public-key to each node. When the sender decided to send the message to node(s) with specific attributes, the sender encrypts the plaintext with an access structure which represents attributes. When the recipient received the ciphertext, the recipient decrypts the ciphertext with attributes. If the recipient satisfied with the access structure of ciphertext, the message will be decrypted. Especially, Attribute-Based Proxy Re-Encryption[4] has a different procedure from attribute-based encryption scheme [3] after step (4). The sender decides to distribute the capability of decryption. It sends a message including attributes for authority of appliances to PKG. Then messages are re-encrypted with visitor attributes in PKG. If PKG receive a request from a visitor, PKG sends the re-encrypted message. The recipient decrypts the message and then obtains attributes which is the capability for authority of appliances.

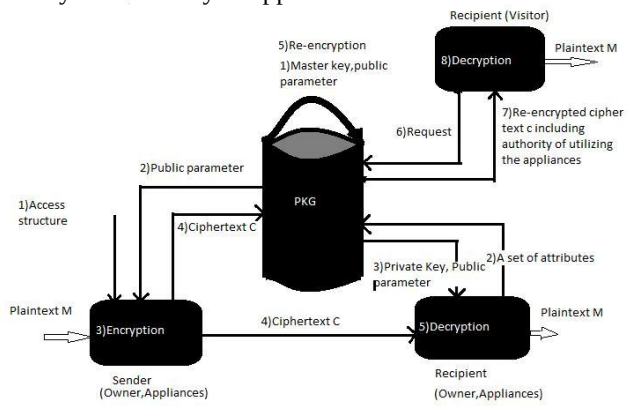

Figure 2.4: Attribute-based proxy re-encryption scheme

2.4.2 Home automation using attribute-based proxy re-encryption

Home automation with ABPRE is more practical method than other schemes. If owner invites his friends to home managed by home automation system, they need to receive an authority for controlling and managing appliances in home automation. In ABPRE, owner can control the capability of management. Visitors cannot control anything in the house because of security policy. For this reason, owner determines to delegate the power to suitable visitors for utilizing the appliances [4].

In the right of fig. 2.5, authority of appliance is extended to visitors. After distribution of attributes, appliances (lights, electronic faucets) are controlled by visitors.

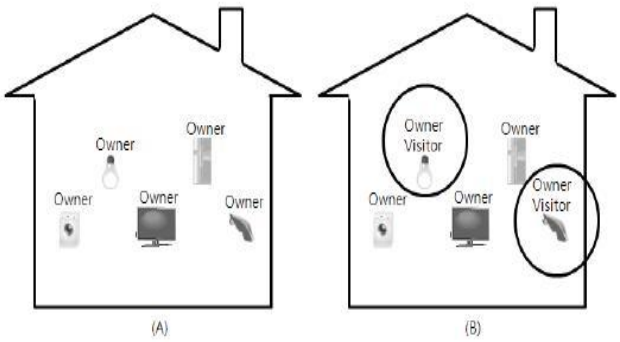

Figure 2.5: Delegation the authority for appliances to visitor : (A) before delegation, (B) after delegation

Owner can set the specific feature depending on circumstances such as some of appliances are not allowed visitor. All of appliances in home can be managed by owner and visitors in APBRE scheme.

III. PERFORMANCE COMPARISON

In this chapter, different approaches for Home Automation using ZigBee are compared based on different parameters. The parameters include :

Number of Keys [1][2][3][4] : ZigBee uses three types of keys. Using these keys, ZigBee network provides secure network. In a full mesh network, each pair of devices share a master key then the number of master keys is $O(n^2)$, where n is the number of network devices.

Digital Signature [1][2][3][4] : Current ZigBee security model doesn't provide digital signature capability. ABE and ABPRE also doesn't offer the digital signature, because they

uses the attributes which is not a representative of the user. However identity based encryption provides digital signature.

Key directory [1][2][3][4] : Identity-based cryptography uses identity of each entity as public key and thus eliminates the need for key directory. Similarly ABE and ABPRE encrypt the message using attributes there by eliminating the need for a key directory. However current ZigBee security requires a key directory to store the master key.

Key escrow [1][2][3][4] : Key escrow (also known as a fair cryptosystem) is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, or governments, who may wish to be able to view the contents of encrypted communications.

Availability of encryption key [1][2][3][4] : The capability of encryption key implies the capability of encrypting a message and sending to a recipient even when that recipient has not obtained his decryption key, which is provided by all approaches other than Current ZigBee security.

Attribute based encryption [1][2][3][4] : In ABE and ABPRE messages are encrypted with user attributes. An attribute based encryption scheme is provided in both cases. However current ZigBee security and identity-based cryptography uses a different approach.

Capability of delegation [1][2][3][4] : Attribute-based proxy re-encryption scheme can re-encrypt the message for delegating the capability of decryption to selected users, which is enabling various services such as simplicity of group key management and delegation of decryption capability. However this capability is not provided by other approaches.

The table 3.1 shows a Comparison of different approaches for ZigBee Security [1][2][3][4].

TABLE 3.1:

A COMPARISON OF DIFFERENT APPROACHES FOR ZIGBEE SECURITY

	Current zigBee Security	IBE	ABE	ABPRE
Number of keys	O(n2)	O(n)	O(n)	O(n)
Digital signature	NO	YES	NO	NO
Digital signature	YES	NO	NO	NO
Key escrow	YES	YES	YES	YES
Availability of encryption key	NO	YES	YES	YES
Attribute based encryption	NO	NO	YES	YES
Capability of delegation	NO	NO	NO	YES

IV. CONCLUSION AND FUTURE WORKS

In this paper different approaches for Home Automation using ZigBee are compared. Comparison is done based on different parameters such as number of keys used in each of the approaches, key directory, key escrow, availability of encryption key in each of the approaches, digital signature etc. Compared to other approaches Attribute-based proxy re-encryption scheme has capability of attribute encryption with specific attributes and re-encrypt the message for delegating the capability of decryption to selected users. ABPRE has a O(n) complexity. Therefore it is the efficient cryptography in terms of distribution and management of keys. However, ABPRE doesn't offer the digital signature, because it uses the attributes which is not a representative of the user.

Also, as a future work, the approaches can be compared in other terms like efficiency of algorithms etc. ZigBee based approaches have a great scope in the field of robotics (ex. robots for home purposes). A new approach based on touch application can also be developed, that includes a pattern recognition unit to recognize certain patterns, such as finger prints of the owner etc.

REFERENCES

[1] C. Ramya, M. Shanmugaraj, and R. Prabakaran, \Study on zigbee technology," In 2011 3rd International Conference on Electronics Computer Technology (ICECT), vol. 6. IEEE, pp. 297{301, june 2007.

[2] S. Nguyen and C. Rong, \Zigbee security using identity-based cryptography," on Autonomic and Trusted Computing, Springer, pp. 3{12, 2007.

[3] H. Seo, C. Kim, and H. Kim, \Zigbee security for home automation using attribute-based cryptography," In 2011 IEEE International Conference on Consumer Electronics (ICCE), IEEE, pp. 367{368, july 2011.

[4] H. Seo and H. Kim, \Zigbee security for visitors in home automation using attribute based proxy re-encryption," In 2011 IEEE 15th International Symposium on Consumer Electronics (ISCE), IEEE, pp. 304{307, july 2011.