Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 10(4): 343-348, Dec. 2012 Regular Paper

ZigBee Security Using Attribute-Based Proxy Re-encryption

Hwajeong Seo and Howon Kim*, ***Member, KIICE***

Department of Computer Engineering, Pusan National University, Pusan 609-735, Korea

Abstract

ZigBee Network is enabling technology for home automation, surveillance and monitoring system. For better secure network environment, secure and robust security model is important. The paper proposes an application, attribute-based proxy re-encryption on ZigBee networks. The method can distribute the authority to designated sensor nodes to decrypt re-encrypted ciphertext with associated attributes. However, a previous method is required to compute complex pairing operations. The high complexity is not suited to low resource device sensor networks, and it does not provide routing security either. To resolve these problems, we present a novel mechanism. The method can reduce overhead by imposing overhead to full function devices and ensure routing paths as well.

Index Terms: Attribute-based proxy re-encryption, Pairing, Sensor network, ZigBee security

I. INTRODUCTION

ZigBee is an enabling technology for various applications including home automation and surveillance systems. ZigBee has the advantages of high availability, low power consumption, and low cost, which is ideal for distributed sensor network environments.

However, security management in ZigBee networking is not at a suitable level for applications because the ZigBee standard security requires a huge capacity for storing master keys, network keys, and link keys between each entity. When the size of the network increases, the number of keys exponentially increases. It also does not offer the flexibility to select the destination nodes, for example.

In this paper, we apply attribute-based proxy re-encryption (ABPRE) [1], which re-encrypts a ciphertext with attributes of the new recipients to delegate the capability of decryption and reduce the number of keys, providing a more practical method. To further reduce the computational complexity, we use a constant pairing operation based on ABPRE [2].

In this work, we present a novel method for ZigBee security. Following are the main contributions of the paper. We present an efficient ZigBee security model and the proposed ABPRE provides a security model that distributes overhead. Finally we show a routing security model using ABPRE.

The paper consists of five sections. In Section II, we introduce related works including ZigBee and ABPRE. In the Section III, we propose the ABPRE model as a ZigBee standard. Section IV includes an evaluation report. Finally, we conclude the paper in Section V.

II. RELATED WORKS

A. ZigBee, Sensor Network Standard

ZigBee is designed to be a low cost, power efficient device and provides effective communication within mesh networks. Therefore, it offers reliable and trustworthy

Received 11 May 2012, **Revised** 16 June 2012, **Accepted** 29 June 2012
***Corresponding Author** E-mail: howonkim@pusan.ac.kr

Open Access **http://dx.doi.org/10.6109/jicce.2012.10.4.343** print ISSN:2234-8255 online ISSN:2234-8883

network services to users.

ZigBee is based on the IEEE 802.15.4 specification and ZigBee standard. IEEE 802.15.4 defines the physical and medium access control layers of the protocol. The higher layers including the network, application support sub-layer, and ZigBee device objects are described by the ZigBee standard.

One of the most interesting features of ZigBee is the possibility of mesh networking. This extends the network range and provides higher network reliability by creation of new paths in case of network configuration changes. If an end device loses its transmission path to the coordinator, it searches for a new path to the coordinator. Therefore, the ZigBee network maintains an appropriate data transmission rate.

B. Security Specification in ZigBee Networks

The ZigBee standard provides data confidentiality by encrypting packets with secret keys using Advanced Encryption Standard (AES) symmetric cryptography.

Three key types are used in ZigBee networks. A master key, which is a long-term security key between two devices, is used for delivery of network and link keys. The second key is a link key, which provides security on the specific link between the two devices. The third key type is a network key used when nodes transmit the information to a member of the network.

Even though ZigBee provides a strong method for protection of information from attackers with symmetric cryptography, ZigBee has restrictions that involve a large number of keys and network keys. In a full mesh network, each node shares each pair of keys with $O(n^2)$ complexity.

C. ABPRE with Constant Pairing Operations [2]

ABPRE with constant pairing operations is an enhanced version of [1]. To reduce the number of pairing operations, exponentiation is conducted instead of the operation. Therefore, the pairing operation is computed at once at the end.

D. Satisfying an Access Structure

In this scheme we consider the access structure consisting of AND gates between positive and negative attributes. Denote the index set of all the attributes as τ. The access structure is represented as $\wedge(+d_i, -d_i)_{i\in\tau}$, which are the positive attribute and the negative attribute, respectively. Any user receives a secret key associated with an attribute set $S \subseteq \tau$ from the authority. The users can decrypt the ciphertext, if the following conditions of the attribute are met:

If $+d_i$ appears in AS, then $i \in S$;
If $-d_i$ appears in AS, then $i \notin S$.

E. Main Construction

SETUP(1^k): A bilinear group G of prime order p, with bilinear map $e: G \times G \to G_T$ is generated. Next, it selects elements $k, y, z, t_i (1 \le i \le 3n)$ in Z_P and two generators g, h of G at random. Let $Y := e(g,h)^y$ and $T_i := g^{t_i}$ for each $(1 \le i \le 3n)$. The public parameter pp includes $< e, g^z, h, Y^{kz}, \{T_i, \frac{t_i}{kz}\}_{1\le i\le 3n} >$. The master key mk is $< k, y, z, \{t_i\}_{1\le i\le 3n} >$.

KGEN (S, mk) Let S denote an index set of attributes. It chooses a random $r_1, \dots, r_n$ from the Z_p and sets $r = r_1 + r_2 + \cdots + r_n$. It computes $\widehat{D} = (h^{y-r})^k$, and for each $i \in N (N = \{1,2,\dots,n\}) (D_{i,1} = h^{r_i})_{i\in N}$. This outputs a user's secret key $usk =< S, (D_{i,1})_{i\in N}, \widehat{D}, kz >$.

ENC (m, AS): Let AS denote an access structure. To encrypt a message $m \in G_T$, it selects a random $s \in Z_p$ and computes $\tilde{C} = mY^{skz}, \hat{C} = g^{sz}$, and $\check{C} = h^{skz}$. For $i \in N$: if $+d_i$ appears as $AS, C_i = T_i^s$; if $-d_i$ appears as AS, $C_i = T_{n+i}^s$; otherwise, $C_i = T_{2n+i}^s$. It outputs $C =< AS, \tilde{C}, \hat{C}, \check{C}, (C_i)_{i\in N} >$.

RKGEN(usk, AS'): Let usk denote a valid secret key consisting of $< S, (D_{i,1})_{i\in N}, \widehat{D}, kz >$ and let AS' denote an access structure. It selects a random $d \in Z_p$ and set $\vartheta = g^d, \widehat{D}' = \widehat{D}$. For $i \in N, D'_{i,1} = D_{i,1} h^d; C'$ is the ciphertext of ϑ under the access structure AS'. It outputs $rk =< S, AS', (D'_{i,1})_{i\in N}, \widehat{D}', kz, C' >$.

REENC (rk, C): Let rk denote a valid re-key consisting of $< S, AS', (D'_{i,1})_{i\in N}, \widehat{D}', kz, C' >$ and C denote a well-formed ciphertext $< AS, \tilde{C}, \hat{C}, \check{C}, (C_i)_{i\in N} >$. This step checks whether S satisfies AS; if not, output error; otherwise, for $i \in N$:

$+d_i$ appears in AS, $T_i = \frac{t_i}{kz}$;

$-d_i$ appears in AS, $T_i = \frac{t_{n+i}}{kz}$.

Otherwise, $T_i = \frac{t_{2n+i}}{kz}$.

It computes $= \frac{1}{\prod_{i\in N} T_i} = \frac{kz}{\sum_{j\in S} t_j} = \frac{kz}{t}$,

$C = \prod_{i\in N} C_i = g^{s\sum_{j\in S} t_j} = g^{st}$ and $D = \prod_{i\in N} D'_i = h^{d+\sum_{i\in N} r_i} = h^{nd+r}$.

Next, it computes $= e(C, D^T) = e(g,h)^{(nd+r)(ksz)}$.

It then computes

$$\bar{C} = e\left(\hat{C}, \hat{D}'\right)E = e(g^{sz}, h^{k(y-r)})e(g,h)^{(nd+r)(ksz)} = e(g,h)^{(kszy)+(ndksz)}.$$

It outputs a re-encrypted ciphertext

$$C_{re} =< AS', \tilde{C}, \bar{C}, \check{C}, C' >.$$

Note that C_{re} can be re-encrypted iteratively. Thus we would obtain $C'_{re} =< AS'', \tilde{C}, \bar{C}, \check{C}, C'' >$ where C'' is obtained from the REENC algorithm with the input of another rk' and C'. The size of the ciphertext and re-encryption times increase linearly.

DEC (C, usk): Let usk denote a valid secret key $< S, (D_{i,1})_{i\in N}, \hat{D}, kz >$. It checks whether S satisfies AS; if not, it outputs error; otherwise, decrypt.

If C is an original well-formed ciphertext consisting of $< AS, \tilde{C}, \hat{C}, \check{C}, (C_i)_{i\in N} >$, for $i \in N$:

$+d_i$ appears in AS, $T_i = \frac{t_i}{kz}$;

$-d_i$ appears in AS,$T_i = \frac{t_{n+i}}{kz}$.

Otherwise, $T_i = \frac{t_{2n+i}}{kz}$.

It computes $T = \frac{1}{\prod_{i\in N} T_i} = \frac{kz}{\sum_{j\in S} t_j} = \frac{kz}{t}$, $C = \prod_{i\in N} C_i = g^{s\sum_{j\in S} t_j} = g^{st}$, and $D = \prod_{i\in N} D_i = h^{\sum_{i\in N} r_i} = h^r$.

Next, it computes $E = e(C, D^T) = e(g,h)^{krsz}$.

It outputs

$$\frac{\tilde{C}}{e\left(\hat{C}, \hat{D}\right)E} = \frac{me(g,h)^{ksyz}}{e(g^{sz}, h^{(y-r)k})e(g,h)^{krsz}} = m.$$

Otherwise, if C is a re-encrypted well-formed ciphertext consisting of $< AS', \tilde{C}, \bar{C}, \check{C}, C' >$, then it decrypts C' using usk and obtains $\vartheta = g^d$.

Then it outputs

$$\frac{\tilde{C}e(\vartheta, \check{C})^n}{\bar{C}} = \frac{me(g,h)^{ksyz}e(g,h)^{ndskz}}{e(g,h)^{(kszy)+(ndksz)}} = m.$$

Otherwise, if it is a multi-time re-encrypted well-formed ciphertext, and then decryption is similar to the above phases.

III. PROPOSED METHOD

The method is based on the [6] process, which proposes the first form of ZigBee security using ABPRE. In the process, firstly, the sender receives the access structure and public parameters from private key generator (PKG). When the sender needs to transmit the plaintext by executing the encryption process, the data is encrypted with the user's attributes and secret keys. If the recipient is located in the same sub-network or the sender has his attributes, the sender directly transmits the packet to the recipient and then the recipient decrypts the packet with his attributes and public parameters. When the recipient is located in the other network or has attributes which are not in the sender, the sender transmits the packet to the base node. The packet is re-encrypted and then is transmitted to the node in the distance. The recipient decrypts the packet with his secret values. If the packet is encrypted several times, the decryption process is also conducted by an equal number of them. The method needs to pass the base node when the recipient is in the other network. Passing the base node, the packet is re-encrypted, which ensures that the packet is transmitted using the right path. The detailed process is depicted in Fig. 1.

In Fig. 2, an example of the scenario is described. When the sender wants to send a message to recipient #1, it directly transmits the ciphertextto the destination after encryption. In the case of recipient #2, the sender transmits the packet to the base node. The base node then re-encrypts the packet using recipient #2's attributes. The re-encrypted data is transmitted to recipient #2 and then the data is decrypted with the attributes of recipient #2.

The detailed process of the algorithm is described in Table 2.

IV.EVALUATION

A. Performance Analysis

The attribute-based proxy re-encryption scheme has the capability of attribute encryption with specific attributes and re-encrypting the message for delegating the capability of decryption to selected users, which enables various features such as the simplicity of group key management and delegation of decryption capability. Comparing the number of keys with other schemes, ABPRE has $O(n)$ complexity, but the current ZigBee system is $O(n^2)$ because in symmetric cryptography all users should maintain the same secret key as the others. Therefore, traditional cryptography is not suitable for ZigBee security, but the proposed method is efficient in terms of distribution and management of keys. However, ABPRE does not offer a digital signature because it uses the attributes that are not representative of the user.

A detailed report is presented in Table 2. For practical application, a proposal is required to reduce the computation cost because the scheme claims high overhead including pairing operations. Currently pairing operations over sensor networks take about 1 second (Table 3). Therefore, it is not practical if many pairing operations are needed. In traditional ABPRE, the pairing operation is conducted by a number of attributes. Therefore, it is infeasible to enable the technology over a sensor network.

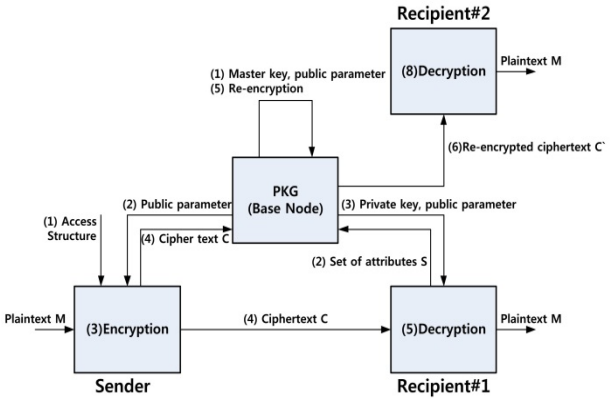

Fig. 1. Process of encryption and decryption. PKG: private key generator.

To solve this drawback, we use a constant pairing operation based on ABPRE [2]. In this method, we must compute two or three pairing operations by conducting decryption. The re-encryption is conducted by a full function node, a base node. Therefore, overhead is reduced in the leaf nodes. Table 4 illustrates the computational complexity of ABPRE. The leaf node needs to conduct the encryption process per each transmission. In the previous method, we had to conduct re-encryption whenever we needed to transmit data to users that were not included in first access structure of the ciphertext by the leaf node. However, in the case of the proposed method, the re-encryption process imposes the overhead on the base node, a much more powerful device. Therefore, the computational costs on the leaf nodes are reduced.

Even though the method provides a small number of pairing operations, it is still not a practical method for ATmega128L and MSP430 devices. The pairing operation over sensor nodes should be improved to perform the proposed method.

Table 1. Process of encryption and decryption over a sensor network

To adjacent nodes
1. Generate a packet
2. Encrypt the packet with its attribute
3. Send the ciphertext to its destination
4. Decrypt the ciphertext
To nodes in the distance
1. Generate a packet
2. Encrypt the packet with its attribute
3. Send the ciphertext to the base node
4. Re-encrypt the ciphertext
5. Send the re-encrypted ciphertext
6. Decrypt the re-encrypted ciphertext

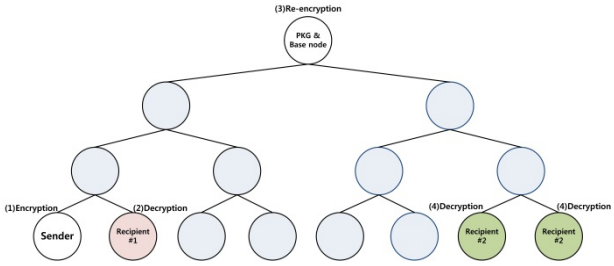

Fig. 2. Architecture of tree network.

B. Security Consideration

The security strength of the proposed model is based on the user's secret key and attributes. First, if the sender's secret key is not revealed to others, the encryption and decryption process are secure, depending on the CTDH and ADBDH assumption. Secondly, the re-encryption process also demands the user's secret key to allow it to proceed. Even though malicious users might obtain the user's encrypted text, they cannot generate a re-encrypted text because the encryption key is not available for malicious users.

Table 2. Performance evaluation of cryptography for ZigBee security [3-6]

Description	Symmetric	Public	Identity	ABPRE
No. of keys in the network	$O(n^2)$	$O(n)$	$O(n)$	$O(n)$
Digital signature, non-reputation	No	Yes	Yes	No
Key directory	Yes	Yes	No	No
Key escrow	Yes	No	Yes	Yes
Availability of encryption key	No	No	Yes	Yes
Attribute-based encryption	No	No	No	Yes
Capability of delegation	No	No	No	Yes

Table 3. Timing table for pairing operations over sensor platform [7]

ATmega128L	MSP430	PXA27X
1.90 sec	1.27 sec	0.14 sec

Table 4. Computational complexity of ABPRE

Encryption	$(n + 2)G_1 + 2G_T$
Decryption	$(3n + 2)G_1 + 2G_T + 2C_e$
Re-encryption	$3nG_1 + G_T + 2C_e$
Re-decryption	$3nG_1 + 4G_T + 3C_e$

ABPRE: attribute-based proxy re-encryption.

V.CONCLUSIONS

In this paper, we propose the novel ABPRE based the ZigBee security model. The method solves the key management problem, provides an attribute-based encryption model, and ensures routing path security. It also has strong features in low cost computation by replacing exponentiation operations for pairing operations and provides a constant number of pairing operations. As a result, the proposed model can be a more practical security model in resource-constrained embedded systems than previous models. However, the method does not show reasonable performance. Future work in faster implementation of the model over various sensor nodes and locating a method for speeding up the model is needed because the current sensor nodes do not show high performance, as described in Table 3.

ACKNOWLEDGMENTS

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (No.2010-0026621).

APPENDIX

Example: Multi-Hop Encryption Model

If sender ‘A’ wants to transmit data to ‘B’ and ‘C’, ‘A’ encrypts the data with attributes of base node ‘1’ and then sends it to ‘1’. Base node ‘1’ sends a ciphertext to ‘2’. First ‘2’ sends the received data to ‘3’ and ‘2’ re-encrypts the data with attributes of ‘B’ and then sends attributes. After receiving the data, ‘3’ also conducts the same procedure, which is computed in base node ‘2’.

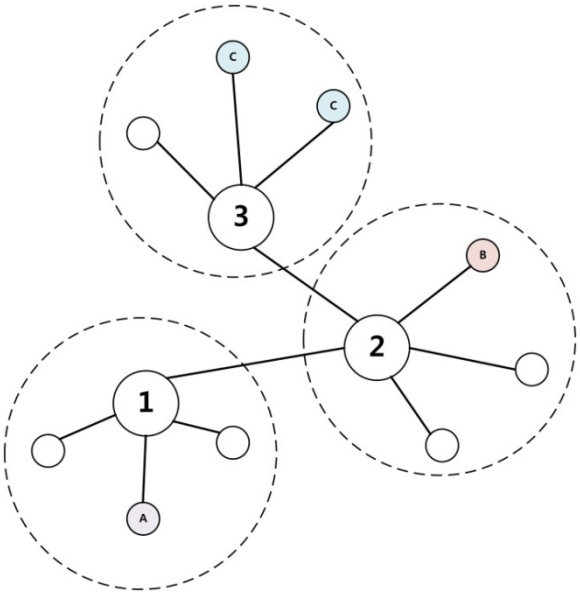

Fig. 3. Multi-hop transmission. Assumption: base node has secret key of leaf nodes.

REFERENCES

[1] X. Liang, Z. Cao, H. Lin, and J. Shao, “Attribute based proxy re-encryption with delegating capabilities,” in *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, Sydney, Australia, pp. 276-286, 2009.

[2] H. Seo and H. Kim, “Attribute-based proxy re-encryption with a constant number of pairing operations,” *Journal of Information and Communication Convergence Engineering*, vol. 10, no. 1, pp. 53-60, 2012.

[3] S. T. Nguyen and C. Rong, “ZigBee security using identity-based cryptography,” *Autonomic and Trusted Computing, Lecture Notes in Computer Science*, vol. 4610, pp. 3-12, 2007.

[4] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” *Advances in Cryptology - CRYPTO 2001, Lecture Notes in Computer Science*, vol. 2139, pp. 213-229, 2001.

[5] H. Seo, C. S. Kim, and H. Kim, “ZigBee security for Home automation using attribute-based cryptography,” in *Proceedings of the IEEE International Conference on Consumer Electronics*, Las Vegas: NV, pp. 364-368, 2011.

[6] H. Seo and H. Kim, “Zigbee security for visitors in home automation using attribute based proxy re-encryption,” in *Proceedings of the 15th IEEE International Symposium on Consumer Electronics*, Singapore, pp. 304-307, 2011.

[7] L. B. Oliveira, D. F. Aranha, C. P. L. Gouvea, M. Scott, D. F. Camara, J. Lopez, and R. Dahab, “TinyPBC: pairings for authenticated identity-based non-interactive key distribution in sensor networks,” *Computer Communications*, vol. 34, no. 3, pp. 485-493, 2011.

Hwajeong Seo
received a BSEE degree from Pusan National University, Pusan, Republic of Korea in 2010, and he received an M.S. degree in computer engineering at Pusan National University. He is in a PhD program in computer engineering at Pusan National University. His research interests include sensor networks, information security, elliptic curve cryptography, and RFID security.

Howon Kim
Received a BSEE degree from Kyungpook National University, Daegu, Republic of Korea, in 1993 and M.S. and Ph.D. degrees in electronic and electrical engineering from Pohang University of Science and Technology (POSTECH), Pohang, Republic of Korea, in 1995 and 1999, respectively. From July 2003 to June 2004, he studied with the COSY group at the Ruhr-University of Bochum, Germany. He was a senior member of the technical staff at the Electronics and Telecommunications Research Institute (ETRI), Daejeon, Republic of Korea. He is currently working as an associate professor with the Department of Computer Engineering, School of Computer Science and Engineering, Pusan National University, Busan, Republic of Korea. His research interests include RFID technology, sensor networks, information security, and computer architecture. Currently, his main research focus is on mobile RFID technology and sensor networks, public key cryptosystems, and their security issues. He is a member of the IEEE, and the International Association for Cryptologic Research (IACR).