Chinese Journal of Electronics
Vol.22, No.3, July 2013

A Security-enhanced Key Distribution Scheme for AODVjr Routing Protocol in ZigBee Networks*

SHANG Tao, HUANG Fuhua, CHEN Jie and LIU Jianwei

(*College of Electronic and Information Engineering, Beihang University, Beijing 100191, China*)

Abstract — ZigBee network is a kind of flexible wireless network technology for control and monitoring applications and new techniques of security measures are essential for high-survivability network. Based on the effectiveness of AODVjr (Ad hoc on-demand distance vector junior) routing protocol in ZigBee networks, in this paper, we proposed a new security-enhanced key distribution scheme for AODVjr routing protocol in ZigBee networks. The key distribution was scheme implemented by combining the parameter exchange of Diffie-Hellman algorithm into the handshake protocol for node's joining a ZigBee network. Especially, the major improvement of Diffie-Hellman algorithm is to mix the parameters of key exchange with XOR operation so as to defend against typical man-in-the-middle attacks. Meanwhile, we analyzed the effect of XOR operation on key parameters by deducing the related theorems. Through the security analysis, the key distribution scheme demonstrates stronger security. We can verify that the AODVjr routing protocol with security enhancement has larger flexible application in ZigBee networks.

Key words — AODVjr, ZigBee, Key distribution, Diffie-Hellman algorithm, XOR operation.

I. Introduction

ZigBee wireless technology based on the IEEE 802.15.4 standard is a kind of flexible wireless network technology, which offers low power consumption, interoperability, reliability and security for control and monitoring applications with low to moderate data rates. The ZigBee Alliance promotes world-wide adoption of ZigBee as the leading wirelessly networked, sensing and control standard for use in consumer electronics, energy, home, commercial and industrial areas, many of which are security sensitive. If the network was not secured, an attacker could modify and inject messages to cause a network error or industrial harm. Meanwhile, many applications also require confidentiality and most have a need for integrity protection.

According to ZigBee Specification[1], the ZigBee stack architecture includes a number of layered components such as IEEE 802.15.4-2003 Physical (PHY) layer and Medium access control (MAC) layer. The ZigBee Alliance builds on this foundation by providing the ZigBee Network (NWK) layer framework for the application layer, which consists of the Application support (APS) layer, the ZigBee device object (ZDO), and manufacturer-defined application objects. For the ZigBee security architecture, the NWK and APS layers are responsible for the secure transport of their respective frames. The APS layer provides services for the establishment and maintenance of security relationships. The ZDO manages the security policies and security configuration of a device. The level of security provided by ZigBee security architecture depends on the safekeeping of symmetric keys, proper implementation of cryptographic mechanism and associated security policies. Trust in security architecture ultimately reduces to trust in the secure initialization and installation of keying material and to trust in the secure processing and storage of keying material. Furthermore it is assumed that secret keys do not become available outside the device in an unsecure way. When a device that has not been preconfigured joins the network, a single key may be sent unprotected, thus resulting in a brief moment of vulnerability where the key could be obtained by any devices. This can lead to a critical security compromise if it is possible for an untrusted device to obtain the key.

To create a highly secured ZigBee network, Sastry *et al.*[2] highlighted a lot of security considerations for IEEE 802.15.4 networks, and Zheng *et al.*[3] presented a systematic analysis of the threats faced by low rate wireless personal area networks with respect to the protocol stack defined by IEEE 802.15.4 and the ZigBee Alliance. Kim *et al.*[4,5] pointed out the difficulty in distributing shared symmetric keys between each pair of nodes, constructed a secure ZigBee scheme for realistic scenarios consisting of a large network with several clusters containing coordinators and numerous devices, and presented an elliptical curve identity-based cryptography protocol to improve the security level of ZigBee network. Chen *et al.*[6] proposed an identity-based authentication protocol for ZigBee networks and designed a secure protocol for exchanging public parameters between two clusters. As a main research direction, routing protocol is important in the context of ZigBee networks and many routing protocols for ZigBee networks have been proposed and proved to be very useful[7−9]. Two

*Manuscript Received Oct. 2011; Accepted June 2012. This work is supported by the Fundamental Research Funds for Central Universities (No.YWF1103Q009), the National Natural Science Foundation of China (No.61272501), and the National Key Basic Research Program of China (No.2012CB315905).

alternative routing schemes were proposed in the framework of the ZigBee Alliance. The first is the well-known AODV (Ad hoc on-demand distance vector) routing protocol, which was designed for highly dynamic application scenarios in wireless ad-hoc networks. The second is a Tree-based routing protocol based on a hierarchical structure established among nodes during the network formation phase. Ran *et al.*[7] introduced the mixed routing strategy of AODV and tree routing of ZigBee and proposed a routing selection strategy based on data services and an energy-balance algorithm in ZigBee. Cuomo *et al.*[8] compared two routing paradigms proposed by the ZigBee Alliance, and pointed that a hierarchical routing scheme based on the MAC association procedures offered more benefits with respect to reactive routing in typical sensor network applications. Qiu *et al.*[9] focused on improving performance in adaptive routing and flexible management for AODVjr routing protocol in a ZigBee network. However, few key distribution schemes for secure routing in ZigBee network have been considered. A malicious node could make use of the flaws and inconsistencies in the routing protocol to create faked routing messages and advertise nonexistent links, provide the incorrect link state information and flood other nodes with routing traffic. Hence the security enhancement of routing protocol for ZigBee networks need be further investigated.

In this paper, to enhance the security of AODVjr routing protocol in ZigBee networks, we focus on the security of routing message and troublesome key distribution problem for ZigBee networks and try to propose an efficient key distribution scheme for secure AODVjr protocol in ZigBee networks. We believe such improvement can enhance ZigBee networks to defend against more attacks.

II. Related Works

ZigBee wireless technology features the formation of Personal area network (PAN): coordinators, routers, and end devices. The coordinator initializes a network, manages network nodes, and stores network node information; the router participates in the network by routing messages between paired nodes; the end device acts as a leaf node in the network. The routing protocol of ZigBee network must consider routing responsibility of different devices. For this reason, AODVjr + Cluster tree routing protocol was used to solve this problem[9]. AODVjr is based on the AODV routing protocol and is a trimmed down AODV specification which removes all but the essential elements of AODV and has nearly the same performance as AODV[10]. Concretely, AODVjr removes the following items from the AODV specification: sequence numbers; gratuitous Route reply (RREP); hop count; hello messages; Route error (RERR); precursor lists. The AODVjr routing protocol is a reactive routing protocol, and routes are determined only when needed. Although source originates route on-demand, the destination, not source, finally determines the route due to the unique resulting route. Then an improved AODVjr with multiple feedback policy was proposed[11]. It can change the routing decision commander from destination to source and make a proactive routing decision on the basis of multiple feedback information.

One immeasurable quality of AODVjr is its simplicity. To enhance the security of AODVjr routing protocol in ZigBee networks, the part of routing information needs to be protected by some secure measure. Since AODVjr has been simplified without hop count, it is not necessary to use hash chains to secure the hop count information. Although RERR messages have a big amount of mutable information, RERR is also not used by AODVjr. Meanwhile symmetric cryptography provides a solution of digital signature with tamper resistant. Therefore every node (generating or forwarding a routing message) uses digital signatures of symmetric cryptography to sign the whole message and any neighbor verifies the signature. Compared with SAODV (Secure AODV)[12], the authentication of our proposed security scheme[13] is to also use digital signatures to authenticate the immutable fields of the routing messages, but not use hash chains to secure the hop count information (the only mutable information in the messages).

A node disseminates a RREQ when it determines that it needs a route to a destination and does not have one available. Each node receiving the request caches a route back to the originator of the request, so that the RREP can be unicast from the destination along a path to that originator. The formats of RREQ and RREP are one part of payload field of ZigBee network frame[1]. The ZigBee network frame is composed of a header and a payload. The header contains the frame control field and an appropriate combination of routing fields as required, while the payload contains information specific to the frame type with variable length. For RREQ or RREP command, the command identifier field will be set to one of the non-reserved values. The command payload field will contain the command itself. The immutable information of routing packets mainly contains the following fields: command identifier, command options, route request identifier, originator address, destination address, responder address. The network address of ZigBee is decided by coordinator. The identification verification can guarantee the correctness of routing message. If the routing message comes from faked node, the routing message will be discarded.

In a ZigBee network, source node S will send a RREQ message to destination node D. The immutable information of RREQ message is denoted by M, k_1 is the distributed key, and I_1 is the first intermediate node. The source node S shares the key k_1 with I_1, while I_1 share another k_2 with next-hop node. When a node sends or receives a routing message, it will use the corresponding key to encrypt or decrypt the immutable information of routing message. Since the receiver and sender share the same symmetric key and the immutable information of routing message is used for cipher, the hop-by-hop identification verification is realized and the security of routing process is guaranteed, just as described in the following part.

$$
\begin{aligned}
&S \rightarrow I_1 : E_{k_1}[M]\\
&I_1 \rightarrow I_2 : E_{k_2}[M]\\
&\cdots\\
&I_{n-2} \rightarrow I_{n-1} : E_{k_{n-1}}[M]\\
&I_{n-1} \rightarrow D : E_{k_n}[M]
\end{aligned}
$$

According to the hop-by-hop identification verification,

each node owns one key for symmetric encryption and another key for symmetric decryption, and the keys between each pair of nodes are different.

The security scheme is based on the following assumption:

(1) All legal nodes join network during the initial period of network construction. Afterwards, the network does not permit a joining request of new node any more, but may revoke request of old node;

(2) All nodes do not join the network at the same time, but in succession.

The first assumption depends on the condition that there not exists any malicious node during the initial period of network construction. This is a strong assumption for practical application. Thus we solve this problem and combine the related solution into our security scheme.

III. Security-enhanced Key Distribution Scheme

We extended the above security scheme with secure key distribution during the initial period of network construction. As a main idea, the key distribution was achieved based on ZigBee network characteristics and improved Diffie-Hellman (D-H) algorithm.

1. Key distribution

In a ZigBee network, a new node usually needs to join the network, and then obtain key for routing message. It is guaranteed that nodes are organized according to Cluster-Tree relationship. In order to distribute key between each pair of nodes, it is convenient to generate key between the network and new node when a node prepares to join a network. The procedure for joining a network using the MAC layer association is initiated by issuing a series of primitives just as shown in Fig.1.

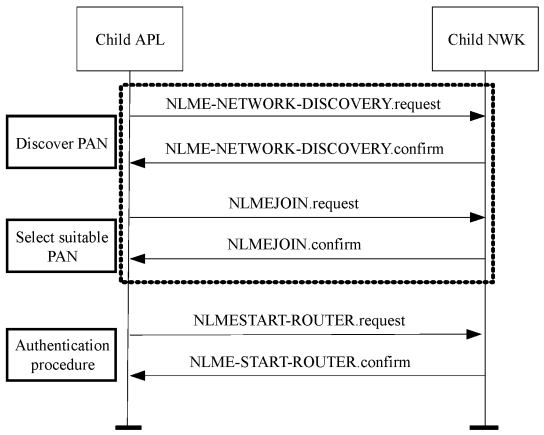


Fig. 1. Procedure for joining a network through association

Considering that during the period of discovering PAN and selecting PAN, hand-shake protocol is necessary for node's joining a ZigBee network, we adopted D-H algorithm for key exchange. D-H algorithm allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. Thus we can combine the parameter exchange of D-H algorithm into the hand-shake protocol for node's joining a ZigBee network.

D-H algorithm exchanges four parameters by two hand-shakes, and joining a ZigBee network also requires two hand-shakes by means of beacon request frame, beacon frame, associate request frame, and associate response frame. Therefore it is feasible to exchange key parameters by means of two hand-shake protocol. By improving the payload field of related frames, the four parameters of $n, g, K_{\mathrm{A}}, K_{\mathrm{B}}$ for key exchange are attached into beacon request frame, beacon frame, associate request frame, associate response frame, respectively.

Concretely, when node A tries to join ZigBee network by node B, (1) it firstly broadcasts a beacon request frame carrying with parameter n. (2) Node B receiving the beacon request frame generates a large prime number g and broadcasts a beacon frame carrying with parameter g. (3) Node A receives the beacon frame carrying with parameter g and identifies the node address sending the beacon frame. According to the received parameter g, the parameter K_{A} can be calculated. Node A sends a associate request beacon carrying with the parameter K_{A} to node B. (4) Node B receives the associate request beacon, calculates the parameter K_{B} and symmetric key, and then broadcasts a associate response frame carrying with parameter K_{B}. (5) Node A receives the associate response beacon, calculates the symmetric key, and successfully joins the network.

In general, the parameters of n and g for D-H algorithm are generated at random, but it is still dangerous to transmit these parameters in a ZigBee network, which could cause two problems: (1) the parameter of plain text is easy to be eavesdropped by malicious attacker; (2) the man-in-the-middle attack can easily happen. Therefore it is a key problem how to transmit parameter for D-H algorithm in a secure way.

Considering the computing advantage of XOR operation, D-H algorithm is improved based on XOR operation of parameters. Here XOR is represented to be $\oplus$.

The improved D-H algorithm includes five steps:

Step 1 Node A generates a random prime number n, and sends n to B;

Step 2 Node B generates a base g, and sends $g \oplus n$ to A;

Step 3 Node A chooses a secret integer X_{A}, restores g by $n \oplus (n \oplus g)$, computes $K_{\mathrm{A}} = g^{X_{\mathrm{A}}} \bmod n$, and sends it to B;

Step 4 Node B chooses a secret integer X_{B}, computes $K_{\mathrm{B}} = g^{X_{\mathrm{B}}} \bmod n$, computes $Key = K_{\mathrm{A}}^{X_{\mathrm{B}}} \bmod n$, and sends $K_{\mathrm{A}} \oplus K_{\mathrm{B}}$ to A;

Step 5 Node A restores K_{B} by $K_{\mathrm{A}} \oplus (K_{\mathrm{B}} \oplus K_{\mathrm{A}})$, and computes $Key = K_{\mathrm{B}}^{X_{\mathrm{A}}} \bmod n$.

Finally node A shares the Key with node B.

2. Theoretical analysis

We discussed the effect of XOR operation on parameters by Theorem 1, Theorem 2, and Theorem 3.

Definition 1 For a binary number, effective bit number is the length from the lowest bit to the highest nonzero bit.

Theorem 1 The result of XOR operation between a large prime number n and a base g is not a prime number with the possibility of $\geq \left(1 - \frac{1}{\lambda}\right)$, where λ is the number of

candidate bases.

Proof XOR operation is a kind of operation on binary format, so a large prime number n and a base g can be represented by the formula (1).

$$n = \sum_{i=0}^{t_n-1}(a_i 2^i), \quad g = \sum_{j=0}^{t_g-1}(b_j 2^j), \quad t_n \geq t_g \geq 2 \tag{1}$$

where t_n and t_g are the effective bit number of the large prime number n and the base g, respectively. Since the minimum prime number is 2, the effective bit number is 2 (the binary format is 10).

Since a prime number except for 2 is also odd number, the large prime number n is denoted by binary format: $a_{t_n-1}\cdots a_1 1$.

Since the base g is a primitive root of the large prime number n, it is also a small prime number. Such small prime number includes 2 and other numbers.

In the case of $g = 2$, the small prime number g is denoted by binary format of 10. For XOR operation,

$$n \oplus g = a_{t_n-1}\cdots a_1 1 \oplus 10 = a_{t_n-1}\cdots a_2 a_1' 1$$

Although a_1' is not a determined value, the result of $n \oplus g$ is definitively an odd number, but not absolutely a prime number.

In the case of $g \neq 2$, the small prime number g is denoted by binary format of $b_{t_g-1}\cdots b_1 1$. For XOR operation,

$$n \oplus g = a_{t_n-1}\cdots a_1 1 \oplus b_{t_g-1}\cdots b_1 1 = a_{t_n-1}\cdots a'_{t_g-1}\cdots a_1' 0$$

Although $a'_{t_g-1}, \cdots, a_1'$ are not determined values, the result of $n \oplus g$ is definitively an even number, and not a prime number.

In general, the number λ of primitive roots is limited ($\lambda \geq 1$). Thus combining the above two cases, the result of XOR operation between a large prime number n and a base g is not a prime number with the possibility of $\geq ((\lambda-1)/\lambda) = \left(1-\frac{1}{\lambda}\right)$.

Remark 1 Since the result of XOR operation between a large prime number n and a base g is probably not a prime number, the faked base g could be easily judged by the prime number property.

Theorem 2 The XOR operation between two numbers is equivalent to mod operation with the priority of larger number, *i.e.*, $P \oplus Q = \max(P,Q) \bmod \min(P,Q)$.

Proof Two numbers P, Q can be denoted by binary format:

$$P = \sum_{i=0}^{t_A-1}(a_i 2^i), \quad Q = \sum_{j=0}^{t_B-1}(b_j 2^j), \quad t_P, t_Q \geq 1$$

where t_P and t_Q are the effective bit number of P and Q, respectively.

If $P \geq Q$, then $t_P \geq t_Q$. Meanwhile, 0 is default bit item for the binary format of a shorter number.

The result of XOR operation between two numbers is

$$P \oplus Q = \sum_{i=0}^{t_P-1}((a_i - b_i)2^i) = P - Q = P \bmod Q \tag{2}$$

If $P < Q$, then $t_P \leq t_Q$.

The result of XOR operation between two numbers is

$$P \oplus Q = \sum_{i=0}^{t_Q-1}((b_i - a_i)2^i) = Q - P = Q \bmod P \tag{3}$$

By combining above two cases, Eqs.(2) and (3) can be represented by (4).

$$P \oplus Q = \sum_{i=0}^{\max(t_P,t_Q)-1}(|a_i - b_i|2^i) = \max(P,Q) \bmod \min(P,Q) \tag{4}$$

It can be simply represented by $P \oplus Q = \max(P,Q) \bmod \min(P,Q)$, which means two different cases of mod operation for two numbers.

Remark 2 The result of XOR operation between a large prime number n and a base g is equivalent to two-case mod operation.

Theorem 3 The result of XOR operation between public key parameters K_A and K_B is a random number.

Proof For D-H algorithm, a large prime number n and a base g are satisfied with the condition that the base g is a primitive root of the large prime number n, $0 \leq X_A, X_B \leq n-1$.

If node A chooses a secret integer X_A, then public key $K_A = X_A \bmod n$.

If node B chooses a secret integer X_B, then public key $K_B = X_B \bmod n$.

The result of XOR operation between public key parameters K_A and K_B is

$$K_A \oplus K_B = (X_A \bmod \mathrm{n}) \oplus (X_B \bmod \mathrm{n}) \tag{5}$$

It can be easily proved by apagoge that the formula (5) does not satisfy associative law for XOR operation and mod operation. According to Remark 2, $K_A \oplus K_B$ is equivalent to two-case mod operation. The XOR result between public key parameters K_A and K_B is related to two-case mod operation, which enhances the random of result. Thus the result is a random number.

3. Scheme evaluation

The security scheme features two characteristics: one is to effectively combine D-H parameter exchange with ZigBee hand-shake protocol, the other is the improvement of D-H algorithm based on parameter XOR.

As a result, the improved hand-shake protocol of joining network makes full use of the characteristics of ZigBee network, implements secure key distribution during the period of network construction, and guarantees that each joining node owns symmetric keys with multiple neighbor nodes.

According to the above hand-shake protocol, we need to further make the related details clear:

(1) Since n and g are random number, different joining nodes probably use different value of n and g.

(2) During the process of joining network, node will construct key pairs with all neighbor nodes in the communication scope. Each node stores a key table for every pair of nodes.

(3) Just as is shown in Fig.2(a), since node I_3 initially broadcasts a beacon request frame for network joining, and probably receives multiple beacon frames from neighbor nodes. According to the hand-shake protocol, node I_3 finally probably receives multiple associated response frames. Considering that

one node belongs to a unique parent node in a ZigBee network, node I_3 will build network associate with the node whose associate response frame firstly arrives. For other received associate response frames, node I_3 only calculates symmetric key for routing.

(4) Just as is shown in Fig.2(b), key distribution will fail if two nodes simultaneously apply to join network. After two nodes broadcast beacon request frames simultaneously, the network node broadcasts the returned beacon frame. Due to the broadcast of beacon frame, the node I_3 applying to join the network cannot judge whether the received beacon frame is sent to itself or not. Consequently the key distribution is mistaken. Thus in order to avoid such problem, node should be guaranteed to join network at intervals, so that key exchange can be achieved successfully.

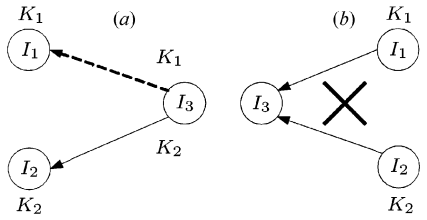


Fig. 2. Design of key distribution process

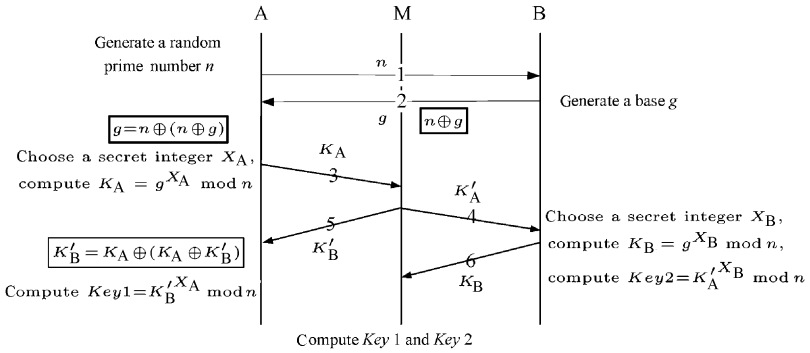


Fig. 3. Typical man-in-the-middle attacks (Blocks denote the new units for improved D-H algorithm)

Table 1. Overall analysis of man-in-the-middle attack

Type	Launching time of attack	Sniffing contents	Malicious action		Result
			Get	Send	
1	After first step	n	n	g'	Attacker is detected
2	After second step	n, $n \oplus g$	n, g	–	More efforts for attacker
3	After third step	n, $n \oplus g$, K_A	n, g, K_A	K'_B K'_A	No shared key is built
4	After sixth step	n, $n \oplus g$, K_A, $K_A \oplus K_B$	n, g, K_A, K_B	–	More efforts for attacker

IV. Security Analysis

The security of the proposed scheme is embodied in D-H defense for network construction phase. We mainly discussed the problem of D-H defense to man-in-the-middle attacks.

For typical man-in-the-middle attacks, as shown in Fig.3, the attacker might completely launch three tasks: (1) obtain the parameter n and g by sniffing; (2) intercept K_A and K_B, then replace them with new K'_A and K'_B; (3) calculate $Key1$ by using K_A and K'_B, and calculate $Key2$ by using K'_A and K_B.

Assume that M is malicious attacker and can obtain all packets after he begins sniffing. According to the launching time of malicious attack, we extend the complexity of man-in-the-middle attacks and discuss the following three cases. The overall analysis is summarized in Table 1.

(1) According to Fig.3, after the first and second steps, M could receive n and $n \oplus g$. Since it does not know the XOR operation of $n \oplus g$, the malicious attacker cannot clearly obtain the parameter n and g. Even if it tries to send a g to A, according to Theorem 1, the faked base g could be easily judged by prime number property. Thus the XOR operation of $n \oplus g$ destroys the first task of man-in-the-middle attacks.

(2) After the third step, M receives K_A. Since it does not know the operation of $g = n \oplus (n \oplus g)$, the malicious attacker is confronted with two cases: M can judge the difference between g and $n \oplus g$ or not.

If M could judge the difference, it would have to stop to analyze the messages of n and $n \oplus g$, try to obtain the correct g. Furthermore, if it could calculate the correct g, M can calculate the effective K'_A and K'_B, and send them to B (the fourth step) and A (the fifth step), respectively. When B sends K_B to M (the sixth step), since M does not know the operation of $K_B = K'_A \oplus (K'_A \oplus K_B)$, it cannot share the key with B. When A obtains K'_B from M, since M does not know the operation of $K_A \oplus K'_B$, M cannot share the key with A. Thus the XOR operation of $K_A \oplus K_B$ destroys the third task of man-in-the-middle attacks.

If M could not judge the difference, M uses wrong base g, so it can not generate correct K'_A and K'_B, and finally cannot share the key with A and B.

(3) After the steps of 1, 2, 3, 6, M can get all data, including n, $n \oplus g$, K_A, $K_A \oplus K_B$. Since it does not know the XOR operation, has to iteratively deduce the internal operation, so this improved D-H algorithm can enhance the security under the condition of no additional computational efforts and memory space.

V. Conclusions

In this paper, we proposed a new key distribution scheme for secure AODVjr protocol in ZigBee networks. Key distribution is based on the ZigBee hand-shake protocol and improved Diffie-Hellman algorithm with higher security. The major improvement is to mix the parameters of key exchange with XOR operation. Such improvement can prevent man-in-the-middle attacks during the period of network formation and false routing information attack during the period of route discovery. Meanwhile we deduced related theorems for function analysis of XOR operation. Despite the performance of network delay might increase, the improved routing protocol necessarily would bring about a better routing security.

References

[1] ZigBee Alliance, ZigBee Specification (R17), 2008.

[2] N. Sastry, D. Wagner, "Security considerations for IEEE 802.15.4 networks", *Proceedings of the 3rd ACM workshop on Wireless security*, Philadelphia, PA, USA, pp.32–42, 2004.

[3] J. Zheng, M.J. Lee, M. Anshel, "Toward Secure Low Rate Wireless Personal Area Networks", *IEEE Transactions on Mobile Computing*, Vol.5, No.10, pp.1361–1373, 2006.

[4] Hyunjue Kim, Chang Hyun Kim, Jong Moon Chung, "A novel elliptical curve ID cryptography protocol for multi-hop ZigBee sensor networks", *Wireless Communications and Mobile Computing*, Vol.12, No.2, pp.145–157, 2012.

[5] Hyunjue Kim, JongChung, Chang Hyun Kim, "Secured communication protocol for internetworking zigbee cluster networks", *Computer Communications*, Vol.32, pp.1531–1540, 2009.

[6] Wei Chen, XiaoShuan Zhang, Dong Tian, Zetian Fu, "An identity-based authentication protocol for clustered ZigBee network", *Proceedings of the Advanced Intelligent Computing Theories and Applications, and 6th International Conference on Intelligent Computing*, pp.503–510, 2010.

[7] Peng Ran, Mao-heng Sun, You-min Zou, "ZigBee routing selection strategy based on data services and energy-balanced ZigBee routing", *Proceedings of the 2006 IEEE Asia-Pacific Conference on Services Computing* (*APSCC'06*), Guang zhou, China, pp.400–404, 2006.

[8] Francesca Cuomo, Sara Della Luna, Ugo Monaco, Tommaso Melodia, "Routing in ZigBee: benefits from exploiting the IEEE 802.15.4 association tree", *Proceedings of IEEE International Conference on Communications 2007*, Glasgow, Scotland, pp.3271–3276, 2007.

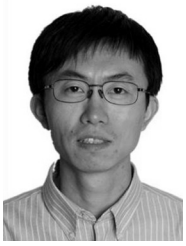
[9] F. Qiu, J.M. Wang, J. Leng, "Design and implementation of a wireless personal area network based on AODVjr routing", *Proceedings of Wireless Mobile & Multimedia Networks*, Beijing: The Institution of Engineering and Technology, London (IET), pp.424–427, 2006.

[10] Ian D. Chakeres, Luke Klein-Verndt, "AODVjr, AODV Simplified", *Mobile Computing and Communication Review*, Vol.6, No.3, pp.100–101, 2002.

[11] Tao Shang, Wei Wu, Xudong Liu, Jianwei Liu, "AODVjr routing protocol with multiple feedback policy for ZigBee network", *The 13th IEEE International Symposium on Consumer Electronics*, Kyoto, Japan, pp.483–487, 2009.

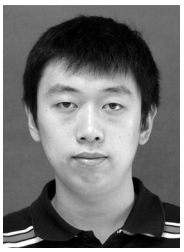
[12] Manel Guerrero Zapata, "Secure Ad hoc on-demand distance vector routing", *Mobile Computing and Communications Review*, Vol.6, No.3, pp.106–107, 2002.

[13] Tao Shang, Jianwei Liu, "Security Enhancement of AODVjr Routing Protocol for ZigBee Network", *The Fifth International Conference on Communications and Networking*, Beijing, China, August 25-27, 2010.



SHANG Tao is an assistant Professor of College of Electronic and Information Engineering at Beihang University, Beijing, China. He received the Ph.D. degree in computer science from Kochi University of Technology, Japan, in 2006, and worked as a postdoctoral in College of Computer Science at Beihang University from 2007 to 2009. His current research interests include wireless network, network coding, and information security. (Email: shangtao@buaa.edu.cn)

HUANG Fuhua received the B.E. degree in electronic and information science and technology from Xiamen University in 2011. He is currently a graduate student at the College of Electronic and Information Engineering, Beihang University, Beijing, China. His current research interests include wireless networks and network coding.



CHEN Jie received the M.E. degree in data communication and computer networks from Northwestern Polytechnical University in 2010. He is currently a graduate student at the College of Electronic and Information Engineering, Beihang University, Beijing, China. His current research interests include wireless networks and information security.

LIU Jianwei is a professor of College of Electronic and Information Engineering at Beihang University, Beijing, China. He received the Ph.D. degree in communication and electronic system from Xidian University, China, in 1998. His current research interests include wireless communication network, coding theory, and information security.