Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/090219

Key Management Mechanism for Authentication Security in Wireless Sensor Network

Ying Wang[1], *Xinguang Peng*[1,*] *and Jing Bian*[1,2]

[1] Colledge of Computer Science and Technology, Taiyuan University of Technology, Shanxi,Taiyuan 030024, China
[2] The Center of Information and Network, Shanxi Medical College of Continuing Education, Shanxi,Taiyuan 030012, China

Received: 21 May 2014, Revised: 20 Aug. 2014, Accepted: 22 Aug. 2014
Published online: 1 Mar. 2015

Abstract: Since the multi-user broadcast authentication protocol in current WSN cannot provide strong safety, perfect scalability and low energy consumption simultaneously. A certificateless key managing scheme based on identity is studied in this paper. The proposed method divides the broadcasting in WSN into two parts: users broadcasting and base station broadcasting. We also adopt different password schemes for system safety. At the user end, a short signature protocol is used for signature and authentication on the broadcasting packet to acquire scalability and low power consumption; at the base station end, partial message recovered Schnorr signature is adopted to protect its broadcasting. In addition, we use the user private protecting scheme based on passwords to resist compromising attacks. Because our improved protocol is based on certificateless signature protocols, it avoids the key escrow problems compared to existing authentication protocols and acquires safety with higher level. The simulations show that the scheme has lowered the power consumption at least 40% without sacrifice in safety and efficiency.

Keywords: Certificateless signature, PKG, Station, Broadcasting authentication, IMBA

1 Introduction

With the development of sensor technologies, the application range of wireless sensor network (WSN) is increasing extensively. WSN is made up of a lot of resources-limited sensor nodes and communicating by wireless link [1,2]. Owing to openness of wireless link, the opponents might initiate various attacks. Establishing pair-wise key between nodes is the basis to realize secure communication of sensor network. Since the resources such as storage capacity, computing capacity, communication bandwidth, node energy, etc, on sensor node itself are limited [3], the key agreement methods in many successfully traditional networks cannot be directly applied. From multi-user broadcasting, there are a lot of users who are WSN data users. They dynamically broadcast towards WSN in order to obtain the latest data [4]. Since WSN may locate in hostile environment, multi-user broadcasting is demanded to provide safeguard to resist malicious attacks. In addition, multi-user broadcasting authentication can satisfy the scalability, that is, new sensor nodes are added in any time to allow users to be dynamically added and revoked [5,6]. However, the data processing ability of WSN nodes is limited and consumed energy is extremely limited. So it is always the research focus to design secure, extensible and efficient multi-user broadcasting protocol for WSN.

With constant improvement of processing performance of sensor nodes, recent schemes incline to adopt public key cryptosystem to make multi-user broadcasting authentication in WSN. Benenson, etc, proposes the first multi-user authentication scheme [7]. Though it is robust, the scheme needs to use public key certificate while public key certificate verification increases sensor nodes times on ECC operation. Public key certificate transmission increases authentication information length to result in efficiency limitation. Reference [8] improves the schemes of Benenson, based on self-verified public key cryptosystem. It combines SC-PKI and symmetric cryptosystem to reduce the energy consumption. The scheme makes authentication with preset public/private pairs in sensor nodes. Attackers are easy to capture sensor nodes and obtain their private keys, so it has deficiency in robustness. Ren, etc, proposes a multi-user authentication scheme HAS with strong robustness [9]. In order to remove the transmission of users' public key certificate, HAS presets the generated

* Corresponding author e-mail: ablewy@163.com

user public key information based on Bloom filter and binary tree in each sensor node. However, since binary tree demands total users as the fixed value, HAS does not satisfy the scalability. Only when old users are revoked, can new users be added in system. To provide perfect scalability, reference [10] proposes an identity-based public key scheme IDS. However, IDS needs a great number of time-consumed bilinear pairings and its energy consumption of scheme is too high. Therefore, reference [11] points that it is still a problem for multi-user broadcasting authentication to simultaneously realize strong security, perfect scalability and high efficiency in WSN. Other works about the security problem in WSN please refer to paper [12]-[20].

Aiming at above problems, this paper proposes an identity-based multi-user broadcasting authentication (IMBA) protocol without key escrow in WSN. It adopts the operation without pairing and the certificateless cryptosystem, to improve multi-user broadcasting authentication protocol. Our scheme has short signature, providing users' broadcasting authentication and simultaneously applies partial message recovered Schnorr signature to provide base station authentication. The presents paper is organized as followsSector 2 is the introduction of network model, attacker model and relative design definition. Sector 3 analyzes identity-based certificateless short signature protocol as well as its implementation in WSN authentication in detail, to prove its performance in security. Then, a certificateless WSN broadcasting authentication scheme is proposed based on the key management mechanism and partial message recovered Schnorr signature. Sector 4 analyzes the work efficiency, communication energy cost and computation consumption of the improved through some experiments. The last sector summarizes the researches in this paper and proposes the perspective in future.

2 Preliminaries

2.1 Network models

Considering the application of WSN in large scale scenes such as environmental monitoring and battlefield test, these kinds of applications usually use a large scale of WSNs and support lots of data users. In such scenes, WSN is composed of lots of resources-limited sensor nodes. Node adopts IEEE 802.15.4 standard [21] which supports variable length load with 102 bytes length. Therefore, enough space is provided for broadcasting messages to carry signatures. The base station in WSN is network deployer which is supposed to be credible. The network supports lots of user nodes and provides monitoring data to them. Users can choose to participate in the network while qualification of violating users' is also revoked. Therefore, the number of users is dynamically changes. Both user and base station can send broadcasting messages and the base station broadcasting is used to manage information such as establishing routing tree and synchronizing information, etc. Users' broadcasting information data is used to collect the latest monitoring data. Therefore, sending messages has stronger processing ability and energy supply in comparison with receiving. Similar to references [22] and [23], the designed protocol in this sector also hypothesizes that WSN has secure time synchronization.

Attacker might modify information of WSN or send false messages. It might also perform compromising attack against users and nodes, or even destroy the whole sensor network by exhausting sensor nodes resources. In order to approach these objects, attacker may act on the basis of following types: Active attack: attacker replays previous effective broadcast messages to control the sensor nodes to perform certain operations. Meanwhile, attackers might also destroy wireless sensor network through modifying messages. Compromising attack: users of wireless sensor network usually use portable equipment for access, which leads that users are easily suffering from compromising attack. Attackers can obtain users' secret information through acquiring users' physical device. They can also impersonate this user and attack sensor network. Attackers can also capture the sensor node to attack sensor network.

2.2 Related definitions

Definition 2.1. $k-CAA$ question: for an integer k and any $s \in Z_q^*$, G is the cyclic additive group whose order is large prime number q, $P \in G$. Given $\{P, sP, e_i \in Z_q^*, i = 1,2,...,k\}$ and $\{\frac{1}{s+e_1}P, \frac{1}{s+e_2}P, ..., \frac{1}{s+e_k}P\}$is used to compute $\frac{1}{s+e}P$. $e \notin \{e_1, e_2, ..., e_k | e_i \in Z_q^*\}$, $\frac{1}{s+e}$ and $\frac{1}{s+e_i}P$ are inversion operations with model q.

So far, $k-CAA$ question is still difficult. It means that effective algorithm cannot be found to solve this problem in polynomial time.

Definition 2.2. Inv-CDH question: Let G be a cyclic additive group and P is a generator of G. For unknown random number $a \in Z_q^*$, given P, aP are used to compute $\frac{1}{a}P$.

Inv-CDH question is equivalent to CDH question in polynomial time, so it is as difficult as CDH.

3 Identity-based key management mechanism and its implementation in broadcasting authentication

3.1 Certificateless short signature protocol

Our improved protocol introduces a private key generator (PKG). It is a credible third party and server at network

initialization, for initializing and key extracting. The algorithm of improved protocol is depicted as follows:

(1) Algorithm initializing: Choosing a safety parameter k and PKG choose group G_1 and G_2 whose orders are prime number$q > 2^k$. Set bilinear pairings $e : G_1 \times G_1 \to G_2$ and P is generator of G_1.Let $g = e(P,P)$. Then PKG select two different Hash functions $H_1 : \{0,1\}* \to Z_q^*$, $H_2 : \{0,1\} * \times G_1 \to Z_q^*$. Choosing a random number $s \in Z_q^*$ as the main key of system and computing the public key $P_{pub} = sP \in G_1$ according to s. Finally PKG will announce the parameter $params = \{k, G_1, G_2, e, q, P, g, P_{pub}, H_1, H_2\}$ and save s secretly.

(2) Extracting algorithm for part of the private keys: According to the stored information in initialization, for $ID \in \{0,1\}*$, PKG computes $Q_{ID} = H_1(ID)$ and $d_{ID} = \frac{P}{s+Q_{ID}}$. Then PKG sends d_{ID} to user whose identity is ID through safety channel. The user can verify the validity of d_{ID} by equation $e(d_{ID}, P_{pub} + Q_{ID}P) = g$. If it is tenable, the user receiving d_{ID} is legal. For simplicity we set $T = P_{pub} + Q_{ID}P$.

(3) Setting secret algorithm: the user with identity ID chooses a random number $r \in Z_q^*$ as secret value. Generation can be easily realized on software platform, or performed by random number generator on hardware.

(4) Setting key algorithm: Given $Params$, users can create own secret r and part of private key d_{ID} received from PKG. So the private key $sk_{ID} = (d_{ID}, r)$ is the pair of above two factors.

(5) Setting public key algorithm: $Params$ and r are input to create public key $pk_{ID} = r(P_{pub} + Q_{ID}P) = rT$. Then it is sent to the node.

(6) Certificateless signature algorithm: the message $m \in \{0,1\}*$ needing signature follows the following operation according to current hour $t_c \in \{0,1\}*$ of the system:

Let

$$h = H_2(m||t_c, pk_{ID}) \tag{1}$$

$$S = \frac{d_{ID}}{r+h} = \frac{P \in G}{(r+h)(s+Q_{ID})} \tag{2}$$

Then the signature of user to message m is S.

(7) Certificateless authentication algorithm: Given $Params$ and message pair (m,S). We verify the following algorithms according to public key stored by the node or contained in the broadcasting data packets:

Let $h = H_2(m||t_c, pk_{ID})$

Accepting signature S and returning 1, when the following equation is tenable:

$$Ver(m, ID, k_{ID}, S) = 1 \Leftrightarrow e(S, pk_{ID} + hT) = g \tag{3}$$

The correctness verifying:

$$\begin{aligned} &S = \tfrac{d_{ID}}{r+h} = \tfrac{P \in G}{(r+h)(s+Q_{ID})} \\ &e(S, pk_{ID} + hT) = e(S, rT + hT) \\ &= e(S, r(P_{pub} + Q_{ID}P) + h(P_{pub} + Q_{ID}P)) \\ &= e(\tfrac{P}{(r+h)(s+Q_{ID})}, (r+h)(P_{pub} + Q_{ID}P)) \\ &= e(\tfrac{P}{(r+h)(s+Q_{ID})}, (r+h)(S + Q_{ID})P) \\ &= e(P,P) = g \end{aligned} \tag{4}$$

Figure 1 depicts the process of PKG, user and normal node to execute different algorithms.

3.2 Safety Proofs

In random oracle models, an algorithm C needs to be acted as challenger's character in order to prove a scheme safety. Meanwhile, the adversary and challenger are needed to play and interact to simulate genuine attacking environment. IMBA protocol in this paper is a certificateless signature protocol. Reference [24] provides a safety model of certificateless cryptosystem and it has two kinds of adversaries:

Opponent of type A: χ^A denotes the third-party attacker and it can replace the public of user freely;

Opponent of type B: χ^B denotes malicious PKG. It owns main key of system but it can not replace the public key of any user;

If the probability of winning in game A and B can be neglected, then we believe the certificateless signature scheme is against existing forgery, under adaptive selecting message attack. The rules of game A and B are referred as reference [25] and the safety of improved protocol can be verified by following two lemmas:

Lemma 1: If opposite χ_1 break the protocol, during this process, χ_1 access $H_i(i = 1,2)$, and part of the private keys resolve oracle model. The times of resolving by private key, requesting by public key and signing are respectively q_{H_i}, q_E and q_S. So there is a (ε', t') algorithm C aiming to solve k-CAA questions with the advantage.

$$\varepsilon' \geq (\varepsilon - \tfrac{1}{2^k})(\tfrac{q_{H_i}-1}{q_{H_i}})^{q_E+q_S+1} \tag{5}$$

In the time

$$t' < t + (2q_{pk} + q_S)t_{sm} + q_S t_{inv} \tag{6}$$

where t_{sm} and t_{inv} denote the time for seeking inversion and scalar quantity when computing G_1.

Lemma 2: Assuming χ_2 breaks the protocol, during this process, χ_2 access $H_i(i = 1,2)$, and part of the private keys resolve oracle model. The times of requesting by public key and signing are $q_{H_i}$and q_{pk}, then there is a

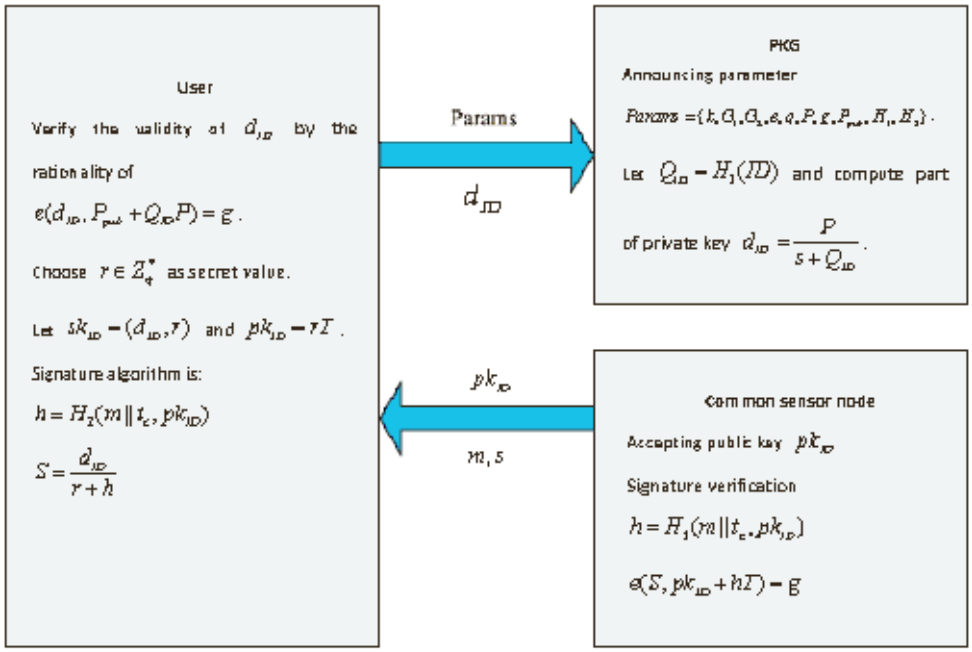

Fig. 1: Executing process of protocol

(ε', t') algorithm C aiming to solve k-CAA questions with the advantage.

$$\varepsilon' \geq (\varepsilon - \frac{1}{2^k})(\frac{q_{H_i}-1}{q_{H_i}})^{q_E+q_S+1} \quad (7)$$

In the time

$$t' < t + (2q_{pk}+q_S)t_{sm} + q_S t_{inv} \quad (8)$$

From lemma 1 and 2 we know, for IMBA protocol and in random oracle models, under the hypothesis of difficult problems k-CAA and Inv-CDH, the probability for adversaries A_1 and A_2 to win can be ignored. IMBA protocol in this sector is anti-existing imitating under adaptively selecting message attack. The safety of IMBA protocol also reflects that it can resist relative attacks. This protocol introduces the credible third party of PKG and hypothesizes it is assumed to be absolutely safe. It stores various ID users' information and generates different partial keys according to different IDs. If one attacker wants to forge a signature, he must obtain private key. But private key is composed by partial key which is provided by PKG and selected by ID users. Therefore, if attacker wants to obtain private key information, he must obtain it from PKG. Under the condition that PKG is absolutely safe the success rate is nearly zero. If attacker cannot obtain private key information, he cannot forge users' signature.

From signature $S=\frac{d_{ID}}{r+h}$ we know that the signature information and users' ID are bounded together. Users with different ID are different for signature of the same message m, so as to realize the function of identity authentication. Thus, it can defend that there are two or more users' broadcasting data packets with the same ID information in network. This identity-based broadcasting authentication protocol effectively guarantees uniqueness of broadcaster's ID and public key. It also prevents that nodes are suffering from Sybil Attack of several different IDs in the same network.

3.3 Multi-user Broadcasting Authentication Scheme

Our scheme is made up by four parts: (1) system initialization: to describe WSN deployment; (2) Users participating: base station generates public or private key for users to dynamically participate in the network. (3) Message broadcasting and authentication: the users or base station broadcasts authentication message for WSN. (4) User revocation: describing process for base station to revoke users. Each part is described as the following steps:

1) System initialization

The base station chooses $(E/F_p, P, q, H_1, H_2)$, the main key and public key of system. The definitions of parameters are the same as described in reference [26].

2) User participating

The user chooses the only identity ID in the whole network, based on which the base station will use private key generating algorithm to create private key pair (R,s).

3) Broadcasting and authentication

When the user owing ID want to broadcast message M to WSN, it sends $\{M,tt,ID,Sig_{ID}\{M,tt,ID\}\}$. tt is current timestamp and Sig_{ID} is the signature to $\{M,tt,ID\}$.

After receiving the message, the sensor nodes will follow the steps:

a) Confirming whether tt is fresh or not;

b) If it is an effective time stamp, the signature is verified or this message is discarded.

c) If signature verification result is false, tt will be discarded or transferred to the next hop.

Since the base station uses Schnorr signature for users to generate private key, while Schnorr signature is more effective than BNN-IBS. Thus, base station still uses Schonorr signature to provide message authentication in broadcastings. Broadcasting messages in base station usually contain specific data such as establishing data of route tree. Thus, base station broadcasting messages usually have larger length. In order to reduce total length of the message, Schnorr signature with message recovery in reference [27] is applied. In order to broadcast message M, the base station perform the following steps:

a) The created broadcasting message is divided into two parts: M_1 and M_2. The length of M_1 is not longer than 10 bytes and M_2 contains $ID_{\sin k}$ and tt;

b) Choosing random number $y \in Z_q^*$ and compute $Y = yP$;

c) Y is performed Hash code operation to create integer i;

d) According to special standard, we add appropriate redundancy to M_1 to create f_1 and compute $f_2 = H_1(M_2)$.

e) Computing $c = i + f_1 + f_2 \bmod q$ to confirm $c \neq 0$, otherwise return to the first step.

f) Computing $d = y - cx \bmod q$ to output (c,d) as signature.

The base station broadcasts message $\{M_2,c,d\}$. When receiving $\{M_2,c,d\}$, the sensor node firs check if the timestamp in M_2 is fresh. If it is then the following steps begin:

If $c \notin [1,q-1]$ or $d \notin [1,q-1]$ the message is discarded.

a) Computing $Q = dP + cP_{pub}$. If $Q = 0$ the message is discarded.

b) Hash code is operated on Q to create integer i

c) Computing $f_2 = H_1(M_2)$ and $f_1 = c - i - f_2 \bmod q$. If the redundancy of f_1 is wrong the message is discarded, otherwise we accept the signature and rebuild message $\{ID_{\sin k},M,tt\} = M_1||M_2\}$

4) User Revocation

If user is discovered to be revoked, this message is discarded. In order to reduce users' compromising attack due to equipments loss, IMBAS will offer password-based private key protection mechanism. Users select password PW first, then compute $s' = H_1(PW) \oplus s$ and store (R,s) at the terminal. Before the private key is used, users will input PWfirst and compute $s = H_1(PW) \oplus s'$ at the terminal. Only when inputting password PW is correct can terminal recover the correct private key (R,s).

4 Performance analysis

4.1 Efficiency analysis

Before the protocol analysis, since the computation cost of Hash operation and Z_q^* inversion is small, we can ignore its influence. IMBA protocol will perform the scalar multiplication on one-time additive group when operating the signature algorithm. It needs to operate one-time scalar multiplication and one-time bilinear pairing during signature verification algorithm. Because EBAP protocol has disadvantages of message length limitations, only the part with partial message recovery function is compared in this experiment. Table 1 shows the efficiency analysis comparison result of EBAP-P, BLS and GS [28,29]. P_r: a bilinear pairing operation; S_m: scalar multiplication on additive group; H_m: a MapToPoint operation; Exp: index operation of EBAP-P on $|G_2|$; $|q|$: bit length of q in binary representation; $|G_1|$the length of each element in $|G_1|$; $|G_2|$: the length of each element in $|G_2|$; $|m_1|$: length of first half of message m_1 in $m = m_1||m_2$.

The length of practical public key and the length of practical signature in table 1 refer to the length obtained by point compression of group G_1 and the length is narrowed to the half. 160 bits group and bilinear mapping on elliptic curve under the premise of offering equalizing 1024 bits RSA security intensity are adopted. It can be seen from table 1, our protocol can approach the minimal 160bits signature length which is the same to BSL. However, its computation complexity is smaller than other protocols. The signature lengths of GS and EBAP-P are too long and the computation complexity is larger than IMBA protocol.

4.2 Computation cost

Since our scheme is similar to IBEKAS and the pair keys of them are all established by exchanging key parameters. The main computation cost differentiates by the computation for exchanging parameters. So we first analyze the complexity of two schemes, as is shown in table 2.

To simplify the analysis, we use the bilinear pairings operation and consumed energy of scalar multiplications on ECC to balance the computation cost. According to research of Chehri, etc. [30], on MICA2 sensor, one scalar multiplication on ECC needs 0.81s and its consumed energy is close to 0; according to research of Bertoni etc. [31], on St22 smart card processor with 32bit and 33MHz, one scalar multiplication needs nearly 0.752s. So the time for bilinear pairings operation on MICA2 sensor is 3.102s and consumed energy is about 74.45mJ. The computation time and energy needed to exchange key parameters between the node and its neighbor nodes are listed in table 3.

Table 1: Comparison of protocol efficiency

Protocol	BLS	GS	EBAP-P	IMBA
Signature	$S_m + H_m$	$2S_m$	$Exp + S_m$	S_m
Verification	$2P_r + H_m$	$3P_r + S_m$	$P_r + Exp + S_m$	$P_r + S_m$
Length of public key	$\|q\|$	$\|G_1\|$	$\|G_2\|$	$\|G_1\|$
Actual length of public key	160	160	171	160
Signature length	$\|G_1\|$	$2\|G_1\|$	$\|G_1\| + \|q\| + \|m_1\|$	$\|G_1\|$
Actual signature length	160	320	$\|m_1\| + 341$[45]	160

Table 2: Analysis on the complexity of two algorithms

Type	IMBA		IBEKAS	
	signature	verification	encryption	decryption
Bilinear pairings			1	1
Hash	1	2	2	1
Scalar multiplication	1	3	1	
Scalar addition		2		
XOR			1	1
Index			1	

Table 3: Comparison of time and energy

Scheme	Time(s)	Energy(mJ)
IMBA	0.81×(3N+1)	19.44×(3N+1)
IBEKAS	(0.81+3.102×2)	(19.44+2×74.45)×N

When the neighbors are different, the computation time and consumed energy are described as figure 2 and figure 3.

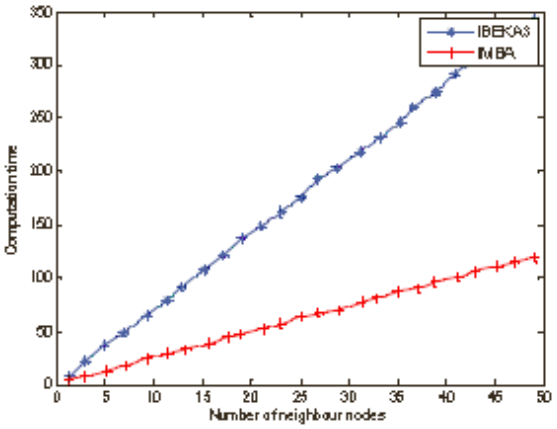

Fig. 2: Comparison of time and energy(Computation time)

From above figures we can see, the consumed computation and energy in this paper is optimal. That is because traditional algorithm adopts scalar multiplication

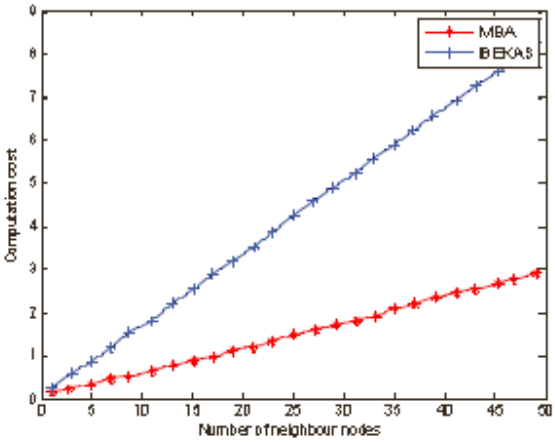

Fig. 3: Comparison of time and energy(Computation cost)

on ECC for signature and authentication. When $N = 40$ and time/energy is 280s/6.744J, the cost is 3 times higher than ours.

4.3 Communication consumption

The decisive factor of communication consumption is the size of message being transmitted. All the algorithms need to send message m except EBAP-P. Then total size of messages is:

$$A = |ID| + |t_c| + |m| + |S| \tag{9}$$

ID is the identity information of broadcaster; t_c is sending time of the packets; *m* is the message and *S* is the signature of *m*. Assuming *ID* occupies 2bytes,$t_c$occupies 2bytes and *m* is 20 bytes and each packet needs 8bytes of booting information, the size of packet in real transmission is:

$$R = 41\left\lfloor \frac{A}{32} \right\rfloor + (A\%32) + 9 + 8(1 + \left\lfloor \frac{A}{32} \right\rfloor) \qquad (10)$$

When using simple flooding routers, each node need one retransmission and receiving w' times of packets. So we get consumed energy of the whole network as:

$$R \times W \times (59.2 + 28.6w') \qquad (11)$$

For the first case we have $A = 44$ bytes. It means two packets are needed totally: 41bytes and 21bytes. From equation 10 we know, the total size of transmitting message is $R = 78$bytes. So consumed energy for receiving message is $78 \times 28.36\mu J \approx 2.23mJ$ and $78 \times 59.2\mu J \approx 4.62mJ$ for sending message. When $w' = 20$, total consumed energy of the nodes is $78 \times (59.2 + 28.6\times)\mu J \approx 49.22mJ$ and $W \times 61.8mJ$ of the whole network.

For the second case we have $A = 64$ bytes. Two packets are needed and total size of transmitting message is 98bytes. The total energy consumed in the network can be computed by equation 11 and $W \times 61.8mJ$.

With the change of number of sensor nodes, consumed energy of each protocol due to communication are shown in figure 4. The energy analysis of BLS, GS and IMBA based on the assumption that public key has been stored in the nodes and it does not need to be transmitted. It can be seen the energy of BLS and GS are higher. Because the signature length of GS protocol is 320bits; BLS needs to send public key message besides the signature. The bandwidth and energy of improved protocol is relatively small and suitable for WSN. But it also has higher demand for storage of nodes when there exists more broadcasting users in network.

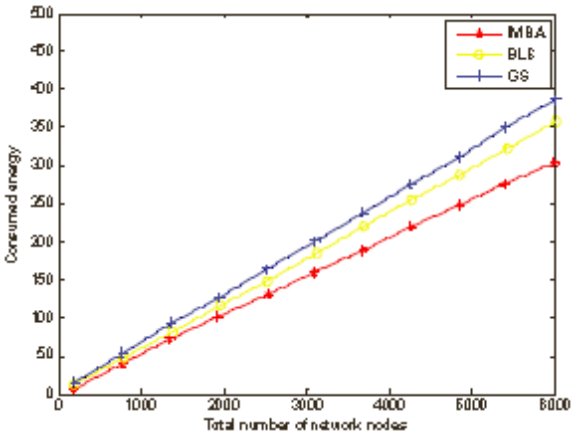

Fig. 4: Comparison of communication consumption

5 Conclusion and future work

This paper mainly studies an identity-based multi-user broadcasting authentication scheme in wireless sensor network. By analyzing the operation of elliptic curve cryptosystem in WSN, it concludes that the point compression technology is not suitable for WSN and the cipher algorithm should have cipher length as short as possible. Then, we propose an identity-based multi-user broadcasting protocol IMBAS in the sensor network. IMBAS adopts an identity-based key management mechanism with new short signature length to protect users' broadcasting, simultaneously it applies partial message recovered Schnorr signature to protect base station broadcasting and provides password-based users' private key protection mechanism to actively resist compromising attack. The experiments prove that our improved scheme realizes multi-user broadcasting authentication in WSN with strong safety, perfect scalability and high efficiency comprehensively.

Since this paper only selects finite numbers of application scenarios to study certificateless public key system. There is large development space for no pairing computation and certificateless implementation. We need study on how to combine certificateless with identity-based cryptosystem, for further research in more wireless network environments.

6 Acknowledgements

This work is supported by the Natural Science Foundation for Young Scientists of Shanxi Province (Grant No. 2012021011-3) Natural Science Foundation of Shanxi Province (rant No. 2009011022-2) and Shanxi Scholarship Council of China (Grant No. 2009-28)

References

[1] Akyildiz IF, Su W, Sankarasubramaniam Y, et al, Wireless sensor networks: a survey, Computer Networks **38**, 393-422 (2002).

[2] Blundo C, Santis A D, Herzberg A, et al, Perfectly secure key distribution for dynamic conferences, information and Computation **146**, 1-23 (1998) .

[3] Yick Jennifer, Mukherjee Biswanath, Ghosal Dipak, Wireless sensor network survey, Computer Networks **52**, 2292-2330 (2008).

[4] Sahoo Prasan Kumar, Hsieh Kun-Ying, Sheu Jang-Ping, Boundary node selection and target detection in wireless sensor network, Proceedings of 4th IEEE and

IFIP International Conference on Wireless and Optical Communications Networks **4**, 100-106 (2007).
[5] Liu Yong-Min, Jiang Xin-Hua, A protocol model for wireless sensor network, Proceedings of International Conference on Networks Security, Wireless Communications and Trusted Computing **2**, 588-591 (2009).
[6] HAN Hong-yan, ZHANG Xi-hong, WANG Wei-guo, WSN's Key Questions and Its Military Applications, Science Technology and Engineering **7**, 1465-1468 (2007).
[7] Z benenson, N Gedicke, O Raivio, Realizing robust user authentication in sensor networks, Proceedings of Real-World WSN **14**, 79-84 (2005).
[8] C Jiang, B Li, H Xu, An efficient scheme for User Authentication in Wireless Sensor Networks, Proceedings of AINAW **7**, 438-442 (2007).
[9] K Ren, W Lou, Y. Zhang, Multi-user broadcast authentication in wireless sensor networks, Proceedings of SECON **7**, 223-232 (2007).
[10] K Ren, W Lou, K Zeng, On broadcast authentication in wireless sensor networks, IEEE Trans. on Wireless Commun **6**, 4136-4144 (2007).
[11] Yuan LingYun, Zhu YunLong, Xu TianWei, Multi-layered energy-efficient and delay-reducing chain-based data gathering protocol for wireless sensor network, Journal of PLA University of Science and Technology **9**, 422-426 (2008).
[12] Khan S. Lloret Jaime, Loo Jonathan, Intrusion Detection and Security Mechanisms for Wireless Sensor Networks, International Journal of Distributed Sensor Networks, Article No. 747483 (2014).
[13] Yoon Min, Jang Miyoung, Kim Hyeong-Il, A Signature-Based Data Security Technique for Energy-Efficient Data Aggregation in Wireless Sensor Networks, International Journal of Distributed Sensor Networks, Article No. 272537 (2014).
[14] Fujimoto Manato, Ozaki Hayato, Suzuki Takuya, Effective Barrier Coverage Constructions for Improving Border. Security in Wireless Sensor Networks, IEICE Transactions on Communications E96B, 3007-3016 (2013).
[15] Rohokale Vandana Milind, Prasad Neeli Rashmi, Prasad Ramjee, Reliable and Secure Cooperative Communication for Wireless Sensor Networks Making Use of Cooperative Jamming with Physical Layer Security, Wireless Personal Communications **73**, 595-610 (2013).
[16] He Daojing, Chen Chun, Chan Sammy, Security Analysis and Improvement of a Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks, IEEE Transactions on Industrial Electronics **60**, 5348-5354 (2013).
[17] Li Chun-Ta, Weng Chi-Yao, Lee Cheng-Chi, An Advanced Temporal Credential-Based Security Scheme with Mutual Authentication and Key Agreement for Wireless Sensor Networks, Sensors **13**, 9589-9603 (2013).
[18] Yu Yong, Ni Jianbing, Sun Ying, Security Analysis of a Distributed Reprogramming Protocol for Wireless Sensor Networks, IEICE Transactions o Information And Systems E96D, 1875-1877 (2013).
[19] Sun Da-Zhi, Li Jian-Xin, Feng Zhi-Yong, The security and improvement of a two-factor user authentication scheme in wireless sensor networks, Personal and Ubiquitous Computing **17**, 895-905 (2013).
[20] Kifayat Kashif, Merabti Madjid, Shi Qi, Component-based security system (COMSEC) with QoS for wireless sensor networks, Security and Communication Networks **6**, 461-472 (2013).
[21] Zhang Ge, Liu Liqiang, Zhou Xiyi, Performance Analysis and Simulation of IEEE 802.15.4 Protocol, Electronic Technology **5**, 76-79 (2011).
[22] YANG Geng,CHENG Hong-bing, An Efficient Key Agreement Scheme for Wireless Sensor Networks, Acta Electronica Sinica **7**, 1389-1395 (2008).
[23] Cai Shao-Bin, Han Qi-Long, Gao Zhen-Guo, Research on cloud trust model for malicious node detection in wireless sensor network, Acta Electronica Sinica **40**, 2232-2238 (2012).
[24] Zhang Z, Wong D, Xu J et al, Certificateless Public-Kev Signature, Security Model and Efficient Construction , Proceeding of the ACNS Applied Cryptography and NetWork Security **2**, 293-308 (2006).
[25] Du H, Wen Q, Efficient and provably-secure certificateless short signature scheme from bilinear pairings, Computer Standards & Interfaces **31**, 390-394 (2009).
[26] Liu Zhi-Xin, Dai Li-Li, Ma Kai, Balance energy-efficient and real-time with reliable communication protocol for wireless sensor network, Journal of China Universities of Posts and Telecommunications **20**, 37-46 (2013).
[27] D Naccache, J.Stern, Signing on a Postcard, Proceedings of Financial Cryptography **10**, 121-135 (2000).
[28] Boneh D, Lynn B, Shacham H, Short signatures from the Weil Pairing, Journal of Cryptology **17**, 297-319 (2004).
[29] FU Xiaojing, ZHANG Guoyin ,MA Chunguang, Survey on Identity-based Key Establishment Protocols for Wireless Sensor Networks, Computer Science **37**, 26-30 (2010).
[30] Chehri Abdellah, Fortier Paul, Tardif Pierre-Martin, A comparison between different FHSS techniques for use in a multiple access secure wireless sensor network, IEEE Wireless and Microwave Technology Conference, **17**, 1178-1185 (2006).
[31] Qi Zheng-Hua, Yang Geng, Ren Xun-Yi, ABE-IBS based signature-encryption method for WSN, Journal on Communications **31**, 37-44 (2010).

Ying Wang is a Ph.D. candidate of the department of computer science and technology at Taiyuan University of Technology. She also serves as lecturer at the department of computer science and technology, Taiyuan University of Technology. Her research interests include computer network and security, trusted computing and cryptography.

Xinguang Peng received his Ph.D. degree in computer application technology from the Beijing Institute of Technology. He also serves as professor at the department of computer science and technology, Taiyuan University of Technology. His research interests include computer network and security, trusted computing.

Jing Bian is a Ph.D. candidate of the department of computer science and technology at Taiyuan University of Technology. Her research interests include network security and data mining.