IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks

Xuefei Cao *, Weidong Kou, Lanjun Dang, Bin Zhao

State Key Laboratory of Integrated Service Networks, Xidian University, P.O. Box 119, 710071 Xi’an, China

Available online 22 October 2007

Abstract

Multi-user broadcast authentication enables a large number of users to join in and broadcast messages to wireless sensor networks (WSN) dynamically and authentically. Public-key-based schemes have been proposed to provide such services; however, none of them achieve security, scalability and efficiency simultaneously. This paper presents IMBAS, an identity-based multi-user broadcast authentication scheme with strong security, sound scalability and efficiency for WSN. IMBAS divides broadcasts into two categories and employs different cryptographic primitives. Users’ broadcasts are secured with vBNN-IBS, a novel pairing-free identity-based signature with reduced signature size, which is proposed in this paper to achieve security, scalability and efficiency; the sink’s broadcast is secured with Schnorr signature with partial message recovery to further optimize the efficiency. Password-based user private key protection is also proposed to resist proactively the compromise attack. Theoretical analysis demonstrates that IMBAS provides strong security and sound scalability. Quantitative energy analysis shows that IMBAS reduces energy consumption by at least 41.5 percent compared with previous identity-based scheme.

© 2007 Elsevier B.V. All rights reserved.

Keywords: Wireless sensor network; Multi-user; Broadcast authentication; Elliptic curve; Identity-based signature

1. Introduction

Wireless sensor networks (WSN) consist of the sink and a large number of randomly deployed sensor nodes which obtain sensed data and route them back to the sink or other data users [1]. WSN enable data collection by means of low-cost sensors, and it can be used in multiple military and civilian applications such as environment monitoring, medical care and system control [2,3]. For WSN, multi-user broadcast is a fundamental communication paradigm [4–6]. In such a paradigm, there will be a large number of users, each user will join in WSN and broadcast messages to the network dynamically in order to query for the latest sensed data. To deploy WSN in a hostile environment, multi-user broadcast authentication is essential to deter against malicious attackers, who try to modify or inject bogus broadcast messages to WSN. Besides security, scalability is another requirement of multi-user broadcast authentication [5]. By scalability, it means that: first, WSN may consist of thousands of sensor nodes and new sensor nodes can be supplemented whenever are needed; second, WSN should be able to support a large number of users, and it should allow dynamic addition of new users as well as easy revocation of misbehaving users [5,6]. However, multi-user broadcast authentication with security and scalability is not easy in WSN because of the resource limitation of sensor nodes. As notified by [5], it is still a wide open problem to find a multi-user broadcast authentication scheme with strong security, sound scalability and efficiency. Therefore, this paper focuses on the design of multi-user broadcast authentication in WSN, which satisfies strong security, sound scalability and efficiency simultaneously.

When the issue of broadcast authentication first appeared, symmetric key cryptography is employed due to its energy efficiency [7–10]. However, symmetric-key-
based solutions are always subject to various attacks, and they are not able to achieve sufficient scalability [11]. Therefore, in this paper, we employ public key cryptography (PKC) to secure the multi-user broadcast in WSN because of PKC’s advantages in security and scalability. Recent study shows that elliptic curve cryptography (ECC) is a suitable PKC candidate for WSN, it is superior to traditional PKC techniques, such as RSA, in terms of short cipher size and low computational cost [12,13]. However, ECC should be applied to WSN with care because its overall energy consumption is still considerably high. Since WSN adopts flooding mechanism in practical broadcast and the data rate in WSN is limited, the message transmission is always energy-consuming [14,15]. Therefore, when ECC is employed in multi-user broadcast authentication, the overall message-attenuator size should be minimized. Furthermore, the transmission of public key certificate should also be avoided because it not only increases the message size drastically, but also introduces extra energy cost for sensor nodes to validate the certificate [5].

Previously proposed broadcast authentication schemes are roughly divided into three categories according to the cryptographic primitives used. Initially, symmetric cryptography has been employed because of their efficiency. However, such schemes [7–10] suffer from weaker security and weak scalability. Schemes in [16,17] are based on another cryptographic primitive called one-time signatures. They are efficient and provide improved scalability. However, such schemes have some limitations, for example, since one-time signature is based on collisions in hash function, the security strength of such scheme will be weakened when more signatures are generated.

Recently, it is a trend to employ PKC to secure the multi-user broadcast in WSN. Benenson et al. proposed the first solution to the problem of multi-user authentication [18]. Their scheme is robust and tested. However, it is not efficient because the user’s public key certificate should be transmitted and verified by sensor nodes. Benenson’s scheme was improve in [19] with self-certified public key cryptography (SC-PKC). This new scheme is efficient because it bases on a novel integration of SC-PKC and symmetric cryptography. However, this solution is not robust enough because every sensor node has to maintain its own public/private key pair, which makes the scheme liable to node compromise attack (or node capture). An attacker may comprise a node and obtain the private key of the sensor by physical capture, then the attacker is able to break the authentication system. Ren et al. proposed a robust multi-user broadcast authentication scheme called HAS based on ECC [4]. To remove the transmission of user public key certificate, HAS preloads each sensor node with user public key information using Bloom filter and Merkle hash tree. However, since the Merkle hash tree requires the total number of users be fixed, HAS does not provide user scalability, a new user can be added to WSN only after the revocation of an old one. An identity-based scheme called IDS [5] was proposed to provide sound scalability. However, IDS is pairing-based, it requires expensive bilinear pairing operations [20], and thus the energy cost of IDS is multiple times higher than that of ECC-based schemes.

In this paper, we propose IMBAS, an identity-based (ID-based) multi-user broadcast authentication scheme in WSN. The main contributions of this paper are:

1. Provide an ID-based multi-user broadcast authentication scheme featured with strong security, sound scalability and efficiency;
2. Propose a variant of BNN-IBS [21] called vBNN-IBS, which is a pairing-free ID-based signature scheme with reduced signature size, for securing users’ broadcasts in IMBAS;
3. Employ Schnorr signature with partial message recovery to secure the sink’s broadcast;
4. Propose a password-based user private key protection mechanism to resist the compromise attack proactively;
5. Present theoretical security analysis as well as quantitative energy estimation to demonstrate the effectiveness of IMBAS.

The remaining part of this paper is organized as follows. In Section 2, we introduce the background cryptographic mechanisms and discuss the implementation of ECC in WSN. Section 3 presents the network model, adversary model and design principles. In Section 4, vBNN-IBS and IMBAS are proposed and described in detail. Theoretical security analysis and quantitative energy evaluation are given in Section 5. Section 6 concludes the paper.

2. Preliminaries

In this section, we first introduce ECC with a discussion of its implementation in WSN; then an ECC-based signature scheme called BNN-IBS is described.

2.1. Elliptic curve cryptography

Let the symbol $E/F_q$ denote an elliptic curve $E$ over a prime finite field $F_q$ defined by an equation $y^2 = x^3 + ax + b$ with $a, b \in F_q$. $A = 4a^3 + 27b^2 \neq 0$ is the discriminant of the equation. $E(F_q)$ denotes the group of points formed by the points on $E/F_q$ and an extra point $O$ called the point at infinity: $E(F_q) = \{(x, y) : x, y \in F_q; (x, y) \in E/F_q \cup \{O\}$. The order of $E(F_q)$ is $m$ and $p$ is a prime number with $p^2|m$. $P \in E(F_q)$ is a point of order $p$ and $\langle G \rangle$ is a group generated by $P$. $\langle G \rangle$ forms a cyclic group under the point addition “+” defined as follows: Let $P, Q \in E(F_q)$, $l$ be the line containing $P$ and $Q$ (tangent line to $E/F_q$ if $P = Q$), and $R$, the third point of intersection of $l$ with $E/F_q$. Let $l'$ be the line connecting $R$ and $O$. Then $P + Q$ is the point such that $l'$ intersects $E/F_q$ at $R$, $O$ and $P + O$. Point multiplication over $E/F_q$ can be computed as follows: $tP = P + P + \cdots + P$. To compute $t$ from a given pair $(tP, P)$ is called elliptic-curve
discrete logarithm problem (ECDLP) and the problem is thought to be intractable. The above introduction of ECC is of a high level of abbreviation and interested readers are suggested to [22] for more details.

Point addition and point multiplication are basic ECC operations. They are very viable to sensor nodes. A standard MICA2 sensor mote can accomplish a point multiplication operation within 0.81 s [13].

Here we discuss the implementation of ECC in WSN. In most applications, to send a point \( Q = (x, y) \), a sender always sends only the \( x \)-component of \( Q \) in order to reduce the communication load. The receiver can then recover the \( y \)-component according to the elliptic curve equation \( y^2 = f(x) \). To compute \( y \) is to compute the square root(s) of \( f(x) \) modulo a large number \( q \), it requires intensive modulo exponential operations. The resulted time complexity approximates that of the ECC point multiplication [23]. For a sensor node, the energy consumption of computing the \( y \)-component is multiple times higher than that of receiving it. Therefore, we believe that the whole ECC point rather than its \( x \)-component should be transmitted in WSN.

### 2.2. BNN-IBS signature scheme

Shamir introduced the concept of ID-based cryptography (IBC) in 1984 [24]. In ID-based cryptosystem, a user’s public key is directly derivable from his/her publicly known identity information, and the user’s private key is calculated by a trusted party, called PKG, i.e. Private Key Generator. A user’s identifier serves as the user’s public key, and the user’s private key is in fact the user’s public key certificate. Therefore, IBS requires no public key certificate and removes the need for certificate transmission and verification.

Since the appearance of IBC, many ID-based signature (IBS) schemes are proposed. An introduction to the available IBS schemes can be found in [25]. However, these schemes are pairing-based, they require the bilinear pairing and removes the need for certificate transmission and verification.

For a sensor node, the energy consumption of computing the \( y \)-component is multiple times higher than that of receiving it. Therefore, we believe that the whole ECC point rather than its \( x \)-component should be transmitted in WSN.

#### Signature Generation

\( A \) signs a message \( m \) with \( \text{Pri}_A \) as follows:

1. Choose at random \( r \in \mathbb{Z}_p \) and compute \( R = rP \).
2. Use system secret key \( x \) to compute \( s = r + cx \), where \( c = H(s|\text{ID}_A||R) \).

#### Signature Verification

A verifier checks a purported signature \( (R, Y, z) \) on message \( m \) given \( A \)’s identifier \( \text{ID}_A \) as follows:

1. Compute \( h = H_z(\text{ID}_A, m, R, Y) \) and \( c = H(s|\text{ID}_A||R) \).
2. Check whether the equality \( zP = Y + h(R + cP_0) \) holds.

The signature is accepted if the answer is \( \text{yes} \) and rejected otherwise.

### 3. Network model, adversary model and design principles

#### 3.1. Network model

In this paper, we consider the WSN application scenario of environment monitoring, which employs a large-scale WSN and supports a great number of, say one thousand, data users. Such a scenario is common in real life. Army protection is an example. In such applications, numerous soldiers, weapons and vehicles may join in and broadcast messages to WSN on any occasion, querying for the latest sensed information of the current battlefield conditions. Another example is the people-centric urban sensing, such as the Active Map application [27], in which all the tourists in a tourist site may compose a WSN. Each tourist carries a small sensing device, acting both as data users and sensors. All the tourists can query information related to the tourist site, such as the shortest way to a certain location or the passenger flow volume there.

In such a scenario, WSN comprise a large amount of sensor nodes with limited resources. Sensor nodes adopt 802.15.4 [28] standard which allows a variable payload of up to 102 bytes. Such a packet provides enough space to include digital signature for broadcast authentication. There is one sink in WSN, it is the WSN’s bootstrapper and is always trustworthy. WSN support a large number of users, to provide all the users with sensed data. The number of users is changing; users can join in WSN dynamically, and will be revoked in case of misbehavior. Message broadcasters include both the sink and users. The sink broadcasts administrative command, e.g. data distributed for routing tree construction or for time synchronization. Users broadcast queries for the latest sensed
data. Compared with sensor nodes, broadcasters are more powerful in terms of computation capability and energy-supply. We also assume that a secure and resilient time-synchronization protocol has been adopted in WSN, the WSN time is loosely synchronized [29].

3.2. Adversary model

The adversaries may modify or inject bogus packets into WSN. They may compromise both network users and WSN nodes. Worse still, they may devastate WSN by exhausting the resources of sensor nodes. To achieve these, the adversary may launch the following attacks:

Active attack: Attackers can replay valid broadcast messages of the previous session, for deceiving WSN nodes to carry out specified actions, such as providing adversaries with sensed data, or adjusting the node’s local timer. Attackers can also modify or directly inject bogus broadcast messages to WSN, causing damage to the network.

Compromise attack: It is very common that WSN users are equipped with portable devices, this makes the WSN users vulnerable to compromise attack [30]. For example, the attackers may physically capture the user’s devices as well as the security information they store. Then attackers may use the compromised users to broadcast to the WSN. Furthermore, attackers may capture sensor nodes, obtain the secret they store, and then use the secret to undermine WSN.

Denial-of-Service (DoS) attack: (a) Attackers may flood bogus packets to WSN, causing WSN nodes to buffer all the messages received. Since the memory is very limited for sensor nodes, such local jamming attack will soon exhaust sensors’ memory and block the subsequent broadcast messages. (b) Compared with the symmetric key operations, the public key operations require sensor nodes more battery power. Attackers may flood arbitrary strings to WSN and deceive sensor nodes to carry out continuous signature verification. This will eventually exhaust the energy of WSN nodes and devastate WSN. Both these two kinds of DoS attacks are more destructive in multi-user scenario because attackers can easily inject more bogus packets.

3.3. Design principles

Given the network model and adversary model above, the design goals of our protocol are as follows:

• Providing robust broadcast authentication so that malicious attackers will be excluded from impersonating legal users, modifying or injecting bogus messages.
• Offering sound scalability.
• Providing user revocation to deter against compromise attack.
• Providing user security information protection so that the chances of attackers to launch compromise attack could be reduced.
• Minimizing the sensor nodes’ energy consumption.

To achieve the above design goals, the design principles behind our scheme are as follows:

• Secure users broadcasts with IBS scheme to provide strong security, sound scalability, and to remove the transmission and verification of user public key certificate.
• Use the ECC-based BNN-IBS scheme to improve computational efficiency; reduce the signature size of BNN-IBS to minimize the communication load.
• Optimize the sink’s broadcast authentication in order to further improve the energy efficiency.
• Protect users’ private keys with user passwords and revoke the compromised user with the sink’s broadcast.

4. IMBAS: ID-based multi-user broadcast authentication scheme

In this section, we first propose vBNN-IBS, a variant of BNN-IBS scheme with reduced signature size, and then propose IMBAS, an ID-based multi-user broadcast authentication scheme.

4.1. vBNN-IBS scheme

BNN-IBS signature is a suitable candidate for WSN because it is ECC-based rather than pairing-based. However, BNN-IBS is not efficient in terms of signature size. A BNN-IBS signature comprises two points over $E/Z_q$ and an integer from $Z_p$. To achieve the same security strength as 1024-bit RSA, the known smallest reachable size of $q$ and $p$ are 168 bits and 166 bits, respectively [31]. Therefore, the resulted signature size is 105 bytes, i.e. $168 \times 2 + 2 + 166$ bits. It will take a sensor node two 802.15.4 packets to carry a BNN-IBS signature. To reduce the signature size, we propose a variant of BNN-IBS called vBNN-IBS. The Setup and User-key Extraction algorithms of vBNN-IBS are the same as those of BNN-IBS. The Signature Generation and Signature Verification algorithms of vBNN-IBS are as follows:

Signature Generation: User $A$ with identifier $ID_A$ signs a message $m$ with its private key $Pri_A = (R,s)$ as follows:

1. Choose at random $y \in Z_p$ and compute $Y = yP$.
2. Compute $h = H_2(ID_A, m, R, Y)$ and $z = y + hs$.

The tuple $(R, h, z)$ is $A$’s signature on $m$.

Signature Verification: Given $(R, h, z)$, $ID_A$ and message $m$, a verifier first computes $c = H_1(ID_A || R)$. Then it checks whether the equation $h = H_2(ID_A, m, R, zP - h(R + cP_0))$
holds. The signature is accepted if it does and rejected otherwise.

Compared with BNN-IBS, vBNN-IBS achieves the same computation complexity with a smaller signature size of 83 bytes. Only one 802.15.4 packet is enough to carry a vBNN-IBS signature. Moreover, vBNN-IBS eliminates the requirements of public key certificate transmission and verification. All these benefit the multi-user broadcast authentication in WSN.

4.2. Description of IMBAS

IMBAS adopts different cryptographic primitives to secure the messages broadcasted by users and by the sink, respectively. The users employ vBNN-IBS to achieve security, scalability and efficiency; the sink adopts Schnorr signature with partial message recovery [32,33] to further improve the efficiency. To cope with compromise attack, IMBAS provides user revocation and password-based user private key protection.

IMBAS consists of four parts: (1) System initialization, in which WSN is initialized; (2) User addition, in which the sink generates a private key pair for dynamically joining users; (3) Message broadcast and authentication, in which a user or the sink broadcasts authenticated messages; (4) User revocation, in which the sink revokes a compromised user. IMBAS is described as follows:

(1) System initialization: The sink chooses \(\langle E/\mathcal{F}_q, P, p, H_1, H_2 \rangle\), system secret key \(x\) and system public key \(P_0\) as described in vBNN-IBS scheme. Each sensor node is preloaded with system parameters \(\langle E/\mathcal{F}_q, P, p, P_0, H_1, H_2 \rangle\).

(2) User addition: A user chooses a unique identifier \(ID\). The sink extracts private key \((R, s)\) based on \(ID\) for the user with the User-Key Extraction algorithm of vBNN-IBS scheme.

(3) Message broadcast and authentication: If a user with identifier \(ID\) wants to broadcast a message \(M\), it sends the following message:

\[
\langle M, tt, ID, \text{Sig}\{M, tt, ID\} \rangle
\]

(1)

where \(tt\) denotes the current time and \(\text{Sig}\{M, tt, ID\}\) is the user’s vBNN-IBS signature over \(\langle M, tt, ID \rangle\).

Upon the receipt of Message (1), a sensor does the following:

(a) Check whether \(tt\) is fresh.
(b) Verify vBNN-IBS signature if \(tt\) is valid, drop the message otherwise.
(c) Reject the message and drop it if the signature verification fails; propagate the message to the next hop otherwise.

Since the sink uses Schnorr signature to generate private key pair for each user and Schnorr signature is more efficient than vBNN-IBS, it will still use Schnorr signature to secure its broadcast. The messages broadcasted by the sink are inclusive of certain data value, such as the data distributed for routing tree construction, hence the message size will be longer. To reduce the overall message size, we combine Schnorr signature with the message recovery technique proposed in [32,33]. Therefore, to broadcast a message \(M\), the sink does the following:

(a) Prepare the broadcast message \(\langle ID_{sink}, tt, M \rangle\) and break it into two parts, \(M_1\) and \(M_2\), where \(|M_1| \leq 10\) bytes and \(M_2\) is inclusive of \(ID_{sink}\) and \(tt\).
(b) Choose at random \(y \in \mathbb{Z}_p\) and compute \(Y = yP\).
(c) Encode-and-hash \(Y\) into an integer \(i\).
(d) Add proper redundancy to \(M_1\) according to certain standard, such as IEEE P1363a Standard [34], and the resulted value is \(f_1\); then compute \(f_2 = H_1(M_2)\).
(e) Compute \(c = i + f_1 + f_2 \mod p\), and make sure that \(c \neq 0\), otherwise go to step (a).
(f) Compute \(d = y - cx \mod p\), and output \((c, d)\) as the signature.

Then the sink broadcasts \(\langle M_2, c, d \rangle\).

Upon receiving \((M_2, c, d)\), a sensor node checks if \(tt\) in \(M_2\) is fresh. If so, it does the following:

(a) Discard the message if \(c \notin [1, p - 1]\) or \(d \notin [1, p - 1]\).
(b) Compute \(Q = dP + cP_0\).
(c) Discard the message if \(Q = \mathcal{O}\).
(d) Encode-and-hash \(Q\) into an integer \(i\).
(e) Compute \(f_2 = H_1(M_2)\), and compute \(f_1 = c - i - f_2 \mod p\).
(f) Discard the message if the redundancy of \(f_1\) is incorrect.
(g) Otherwise accept the signature and reconstruct \(\langle ID_{sink}, tt, M \rangle = M_1 || M_2\).

(4) User revocation: To revoke a user, the sink broadcasts a message for publishing the identity of the revoked user. Sensor nodes listen to the sink’s broadcast and establish the local revocation list. If a sensor node receives a broadcast message from a user whose identity is contained in the revocation list, the sensor node will drop the message.

To reduce the chances of a user being compromised due to physical device capture, IMBAS provides a password-based private key protection for users. A user first chooses a password \(PW\), and then computes \(R = H_1(PW)^{-1}R\) and \(s' = H_1(PW)^{-1}s\). \((R', s')\) is stored into the user’s physical device instead of \((R, s)\). If the user wants to use the private key pair, he/she should first key in \(PW\). \((R, s)\) will be recovered from the stored \((R', s')\) only when the correct \(PW\) is provided.

5. Scheme analysis

5.1. Security analysis

IMBAS employs vBNN-IBS to secure user message broadcast, as for the security of vBNN-IBS, we have the following theorem:
Theorem 1. If BNN-IBS is existential unforgeable, then vBNN-IBS is existential unforgeable.

Proof. Suppose an adversary $A$ can forge a valid vBNN-IBS tuple $(R, h, z)$ on message $m$ and identity $ID$ with probability $\varepsilon$ within time $t$ without ID's corresponding private key pair. Then $A$ can forge a valid BNN-IBS tuple $(R, Y, z)$ on message $m$ and identity $ID$ with probability $\varepsilon$ within time $t + 3t_m + 2t_a$, where $t_m$ is the time to compute a point multiplication in $E(F_p)$ and $t_a$ is the time to compute a point addition in $E(F_p)$.

If $A$ outputs a valid vBNN-IBS signature $(R, h, z)$ with $m$ and $ID$, then $A$ computes $Y = zP - h(R + H_3(ID)||R)P_0$ and outputs $\sigma' = (R, Y, z)$ as a forged BNN-IBS signature. $\sigma'$ will be a valid forged BNN-IBS signature, if the following verification equation holds:

$$zP = Y + H_2(ID, m, R, Y)(R + H_1(ID)||R)P_0$$

(1)

Substituting $Y$ into Eq. (1), we have:

$$h(R + H_1(ID)||R)P_0) = H_2(ID, m, R, zP - h(R + H_1(ID)||R))P_0)$$

Since $(R, h, z)$ is a valid vBNN-IBS signature, then $h = H_2(ID, m, R, zP - h(R + H_1(ID)||R))P_0)$ holds, therefore Eq. (1) holds. To output a forged BNN-IBS given a forged vBNN-IBS tuple, $A$ has to carry out three point multiplications and two point additions in order to obtain $Y$, which results in a forge time of $t' \leq t + 3t_m + 2t_a$. \qed

Now we consider the security strength of IMBAS.

1. **Active attack**: IMBAS employs vBNN-IBS to secure the message broadcasted by users, and vBNN-IBS is existential unforgeable. The message broadcasted by the sink is secured by Schnorr signature with partial message recovery, which is proven secure in [32, 33]. Therefore, it is impossible for an attacker to inject bogus packets or modify a broadcasted message. Timestamp $tt$ is included in the broadcasted message, so it is impossible for an attacker to launch a replay attack.

2. **Compromise attack**: IMBAS provides a reactive method to deter against user compromise attack. When a user is found to be compromised, the sink will revoke the user by broadcasting a revocation message to whole WSN. In addition, to resist the compromise attack proactively, a user protects its private key pair with a password $PW$. Even if an attacker could capture a user’s device, it can only know the encrypted user private key pair $(R', s')$. If the attacker has no idea of the user’s password $PW$, to compute $(R, s)$ from the stored $(R', s')$ is as hard as to solve the ECDLP. Therefore, IMBAS reduces the chances of compromise attack because it is impossible for an attacker to compromise a user by just capturing the user’s device. Since only the system public key is stored in a sensor node, an attacker cannot compromise sensor node by capturing it. If the attacker can obtain the corresponding system secret key from the system public key stored in a sensor, then it can solve the ECDLP. To conclude, IMBAS is robust to both user and node compromise attack.

3. **DoS attack**: IMBAS can resist the local jamming DoS attacks because the issue of authentication delay inborn with symmetric-key-based schemes is precluded in IMBAS by signature verification. A sensor node is able to authenticate a broadcast packet immediately after receiving it. The forged broadcast packet will be dropped after signature verification rather than be stored or forwarded to the next hop. When an adversary floods forged packets to WSN, sensor nodes that are physically closer to the adversary can thus be depleted because they have to carry out continuous signature verification. However, this attack can be mitigated in IMBAS by limiting the times of verification failure. If a sensor node fails to validate the received broadcast packets to a threshold times in a row, it will report the event to the sink. Then the sink will take further actions to investigate the attacker, limit its access to the WSN and take corresponding remedy actions that are outside the scope of this paper.

4. **Scalability**: IMBAS realizes sound scalability based on vBNN-IBS. Receiver scalability is satisfied, because IMBAS can support a large number of sensor nodes, and new sensors can be supplemented to WSN after being preloaded with system parameters when, for example, old sensors run out of energy. IMBAS also provides user scalability. A user can join in WSN dynamically by querying the sink for a private key pair. Given a 2 bytes user ID, the system can support up to 65,535 users.

5.2. Quantitative performance analysis

In the remaining part of this section, we compare quantitatively the performance of IMBAS with that of the previous protocols in terms of the energy consumption and the cost of scalability. We compare IMBAS with HAS [4] and IDS [5] because the three schemes are of the same level of security.

MICA2 motes are widely used in WSN-based environment monitoring applications [35], therefore we assume that the sensor node in WSN with 1000 users be typical MICA2 mote, which works at 8 MHz with a 8-bit processor ATmega128L, and which adopts IEEE 802.15.4 standard. The power level of MICA2 is 3.0 V, the current draw in active mode is 8.0 mA, the receiving current draw is 10 mA, the transmitting current draw is 27 mA, and the data rate is 12.4 kbps [14, 35]. It takes such a MICA2 0.81 s to carry out a point multiplication over elliptic curve [13]. According to [20], the computation of Tate pairing on a 32-bit ST22 smartcard processor at 33MHz needs 0.752 s. It can then be estimated roughly that it takes a MICA2 mote 3.102 s to compute a Tate pairing. The point multiplication and pairing operation are the most time-consuming operations in broadcast authentication. Therefore, we only consider the time for these two kinds
of operations in our evaluation. We use $N$ to denote the number of neighbor nodes to a sensor node.

In IMBAS, for a user to broadcast a message, since vBNN-IBS signature is 83 bytes in size, therefore the message of form $(I)$ is 97 bytes, assuming $M$ is 10 bytes, $ID$ 2 bytes and $r$ 2 bytes. One 802.15.4 packet is enough to carry the payload. A MICA2 mote needs to transmit up to 128 bytes in the physical layer, including an additional 31 bytes packet header [28]. Hence, the energy consumption on transmitting Message $(I)$ is $3.0 \times 27 \times 128 \times 8/12,400 = 6.689 \text{ mJ}$. The energy consumption on message receiving is $3.0 \times 10 \times 128 \times 8/12,400 = 2.477 \text{ mJ}$. To broadcast Message $(I)$ to the whole WSN, a sensor node has to retransmit once and receive $N$ times the same message. The resulted communication energy consumption of a sensor node is $(6.689 + 2.477N) \text{ mJ}$. Now we analyze the computation energy cost. The dominant operation to verify a vBNN-IBS signature is three point multiplications, and the resulted computational energy consumption of a sensor node is $65.009 + 2.477N \text{ mJ}$. When the message is broadcasted by the sink, the overall energy consumption of a sensor node is $42.904 + 1.490N \text{ mJ}$. Suppose the user broadcast happens at a probability of $\lambda$ and the probability for the sink broadcast is $1 - \lambda$, then the average energy consumption of IMBAS is $42.904 + 22.105\lambda + 0.9872N + 1.490N$.

As for HAS [4], to support 1000 users, the auxiliary authentication information as well as the user’s public key should be transmitted, and the resulted energy consumption is $51.317 + 4.606N \text{ mJ}$. With IDS, a sensor node has to carry out two pairing operations, and the overall energy consumption is $154.488 + 2.071N \text{ mJ}$. Fig. 1 illustrates these broadcast energy consumptions as a function of neighborhood density $N$.

Then, based on the above result, we evaluate the lifetime of IMBAS, HAS and IDS, respectively. An ordinary miniature coin-battery contains a charge of 300 mAh, and only a certain fraction, e.g., 10%, of the overall battery capacity is available for security operations [14]. When $N$ is 20 and $\lambda$ is 0.7, MICA2 motes can run 3176 times of IMBAS, 2340 times of HAS and 1653 times of IDS before exhausting their energy sources. The above lifetime evaluation seems promising because only 10% of the overall battery capacity is used by broadcast authentication, and the remaining 90% of the energy can be consumed by other sensing tasks (e.g., data collection and listening to wireless channel).

Finally we compare the cost for scalability of IMBAS with HAS and IDS. The comparison result is provided in Table 1. To support numerous users, HAS preloads a bloom filter vector and a counting bloom filter vector at each sensor node. The resulted storage overhead per sensor is 4.9 KB. When a new user is added, the sink should update all the sensors’ local bloom filter vectors accordingly by broadcasting. Assume the neighborhood density is 20, the energy consumption for user addition is 72.704 mJ. Note that HAS only satisfies partial scalability, a new user can be added only after the revocation of an old user. Both IMBAS and IDS support sound scalability. When a new user is added, no cost is resulted for sensor nodes. When a user is revoked, sensor nodes have to authenticate the sink’s broadcasted revocation message, hence the energy consumption of IMBAS and IDS are 72.704 mJ and 195.908 mJ, respectively.

We draw the following conclusions based on above comparisons. IMBAS provides stronger scalability than HAS. Moreover, IMBAS is more efficient than HAS when neighborhood density is greater than 5, and such a condition holds for most applications in practice. When neighborhood density is 20 and network users takes 70% of the overall broadcast, the difference of energy cost between IMBAS and IDS reaches 36.441 mJ, and the difference will be enlarged with the decrease in user broadcast probability or increase in neighborhood density. Compared with IDS which provides the same level of scalability, IMBAS is more efficient. The energy reduction of IMBAS achieves 41.5%, or 81.359 mJ even in the worst case when all the messages are broadcasted by users. The reasons for these improvements are: (1) The users’ broadcast messages are secured by vBNN-IBS, which is ECC-based rather than pairing-based; (2) The sink’s broadcast message is secured by Schnorr signature, which further reduces the computation complexity; (3) IMBAS minimizes the broadcast traffic by means of vBNN-IBS and the partial message recovery. The above evaluation is carried out on MICA2 mote, which aims at the applications related to environment monitoring. In other applications where time-critical data such as video and vibration are to be collected and trans-

Table 1

<table>
<thead>
<tr>
<th>$N$ (Neighborhood density)</th>
<th>Storage overhead per sensor (KB)</th>
<th>Energy cost of user addition (mJ)</th>
<th>Energy cost of revocation (mJ)</th>
<th>Scalability</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAS</td>
<td>4.9</td>
<td>72.704</td>
<td>72.704</td>
<td>Partial</td>
</tr>
<tr>
<td>IDS</td>
<td>0</td>
<td>0</td>
<td>195.908</td>
<td>Total</td>
</tr>
<tr>
<td>IMBAS</td>
<td>0</td>
<td>0</td>
<td>72.704</td>
<td>Total</td>
</tr>
</tbody>
</table>
mitted, WSN with high data rate will be required. According to [36], MICAz mote can provide a data rate up to 250 kbps. In such scenario, computation accounts for the main part of energy cost. As a result, IMBAS reduces the energy consumption to an even higher percentage, 60.1%, compared with IDS. Compared with HAS, given $N$ of 20 and user broadcast probability $\lambda$ of 0.7, IMBAS consumes 8.380 mJ more than HAS because it requires one more point multiplication than HAS, but this difference will shrink with an increase in $N$ or a decrease in $\lambda$. Since IMBAS is superior to HAS in terms of scalability which is more important to multi-user broadcast authentication, such a cost in energy consumption seems reasonable. Moreover, because IMBAS provides stronger scalability, this problem can be solved easily by adding new sensor nodes to WSN when old ones run out of energy. Another possible solution might be the use of sensor nodes powered by solar battery.

6. Conclusion

In this paper, we propose IMBAS, an ID-based multi-user broadcast authentication scheme in WSN. First, we discuss the implementation of ECC in WSN in Section 2.1. Then a new ECC-based IBS scheme with reduced signature size called vBNN-IBS is proposed. After that, we come up with IMBAS based on a novel integration of the new vBNN-IBS and Schnorr signature with partial message recovery. A password-based user private key protection method is also proposed for IMBAS to deter against the compromise attack proactively. A theoretical security analysis, as well as a quantitative energy evaluation are given in details, showing that IMBAS satisfies strong security, sound scalability and efficiency simultaneously.

IMBAS is suitable for WSN-based environment monitoring applications, such as army protection and Active Map, where there is a large number of data users. In the future, we will focus on the implementation of IMBAS on benchmarks such as TinyOS and finally apply it to practice.

Acknowledgements

The authors wish to thank the editor and anonymous reviewers for their constructive comments that have helped to improve this paper greatly. This work is supported by the National Natural Science Foundation of China (NSFC) Grant 90304008 and the College and University Subject of Doctors Specific Scientific Research Foundation of China (CUDSFC) Grant 2004071001.

References


Below is given annual work summary, do not need friends can download after editor deleted!!!!!!
Welcome to visit again

XXXX annual work summary

Dear every leader, colleagues:

Look back end of XXXX, XXXX years of work, have the joy of success in your work, have a collaboration with colleagues, working hard, also have disappointed when encountered difficulties and setbacks. Imperceptible in tense and orderly to be over a year, a year, under the loving care and guidance of the leadership of the company, under the support and help of colleagues, through their own efforts, various aspects have made certain progress, better to complete the job. For better work, sum up experience and lessons, will now work a brief summary.

To continuously strengthen learning, improve their comprehensive quality. With good comprehensive quality is the precondition of completes the labor of duty and conditions. A year always put learning in the important position, trying to improve their comprehensive quality. Continuous learning professional skills, learn from surrounding colleagues with rich work experience, equip themselves with knowledge, the expanded aspect of knowledge, efforts to improve their comprehensive quality.

The second Do best, strictly perform their responsibilities. Set up the company, to maximize the customer to the satisfaction of the company’s products, do a good job in technical services and product promotion to the company. And collected on the properties of the products of the company, in order to make improvement in time, make the products better meet the using demand of the scene.

Three to learn to be good at communication, coordinating assistance. On-site technical service personnel should not only have strong professional technology, should also have good communication ability, a lot of a product due to improper operation to appear problem, but often not customers reflect the quality of no, so this time we need to find out the crux, and customer communication, standardized operation, to avoid customer’s mistrust of the products and even the damage of the company’s image. Some experiences in the past work, mentality is very important in the work, work to have passion, keep the smile of sunshine, can close the distance between people, easy to communicate with the customer. Do better in the daily work to communicate with customers and achieve customer satisfaction, excellent technical service every time, on behalf of the customer on our products much a understanding and trust.

Fourth, we need to continue to learn professional knowledge, do practical grasp skilled operation. Over the past year, through continuous learning and fumble, studied the gas generation, collection and methods, gradually familiar with and master the company introduced the working principle, operation method of gas machine. With the help of the department leaders and colleagues, familiar with and master the launch of the division principle, debugging method of the control system, and to wuhan Chen Guchong garbage power plant of gas machine control system transformation, learn to debug, accumulated some experience. All in all, over the past year, did some work, have also made some achievements, but the results can only represent the past, there are some problems to work, can’t meet the higher requirements. In the future work, I must develop the oneself advantage, lack of correct, foster strengths and circumvent weaknesses, for greater achievements. Looking forward to XXXX years of work, I’ll be more efforts, constant progress in their jobs, make greater achievements. Every year I have progress, the growth of believe will get greater returns, I will my biggest contribution to the development of the company, believe in
yourself do better next year!

I wish you all work study progress in the year to come.