Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks

Huang Lu, *Student Member, IEEE*, Jie Li, *Senior Member, IEEE*, Mohsen Guizani, *Fellow, IEEE*

Abstract—Secure data transmission is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. In this paper, we study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. We propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. We show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols. The results show that, the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

Index Terms—Cluster-based WSNs, ID-based digital signature, ID-based online/offline digital signature, secure data transmission protocol.

1 I

A wireless sensor network (WSN) is a network system comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and motion. The individual nodes are capable of sensing their environments, processing the information data locally, and sending data to one or more collection points in a WSN [1]. Efficient data transmission is one of the most important issues for WSNs. Meanwhile, many WSNs are deployed in harsh, neglected and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings [2]. Secure and efficient data transmission is thus especially necessary and is demanded in many such practical WSNs.

1.1 Background and Motivations

Cluster-based data transmission in WSNs, has been investigated by researchers in order to achieve the network scalability and management, which maximizes node lifetime and reduce bandwidth consumption by using local collaboration among sensor nodes [3]. In a cluster-based WSN (CWSN), every cluster has a leader sensor node, regarded as cluster-head (CH). A CH aggregates the data collected by the leaf nodes (non-CH sensor nodes) in its cluster, and sends the aggregation to the base station (BS). The LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol presented by Heinzelman *et al*. [4] is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. In order to prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensor nodes in the network, in rounds. LEACH achieves improvements in terms of network lifetime. Following the idea of LEACH, a number of protocols have been presented such as APTEEN [5] and PEACH [6], which use similar concepts of LEACH. In this paper, for convenience, we call this sort of cluster-based protocols as LEACH-like protocols. Researchers have been widely studying CWSNs in the last decade in the literature. However, the implementation of the cluster-based architecture in the real world is rather complicated [7].

Adding security to LEACH-like protocols is challenging, because they dynamically, randomly and periodically rearrange the network's clusters and data links [8]. Therefore, providing steady long-lasting node-to-node trust relationships and common key distributions are inadequate for LEACH-like protocols (most existing solutions are provided for distributed WSNs, but not for CWSNs). There are some secure data transmission protocols based on LEACH-like protocols, such as SecLEACH [8], GS-LEACH [9] and RLEACH [10]. Most of them, however, apply the symmetric key management for security, which suffers from a so-called orphan node problem [11]. This problem occurs when a node does not share a pairwise key with others in its preloaded key ring. In order to mitigate the storage cost of symmetric keys, the key ring in a node is not sufficient for it to share pairwise symmetric keys with all of the nodes in a network. In such a case, it cannot participate in any cluster, and therefore, has to elect itself as a CH. Furthermore, the orphan node problem reduces the possibility of a node joining with a CH, when the number of alive nodes owning pairwise keys decreases after a long-term operation of the network. Since the more CHs elected by themselves, the more overall energy consumed of the network [4], the orphan node problem increases the overhead of transmission and system energy consumption by raising the number of CHs. Even in the case that a sensor node does share a pairwise key with a distant CH but not a nearby CH, it requires comparatively high energy to transmit data to the

- *H. Lu is with the Department of Computer Science, University of Tsukuba, Tsukuba, Japan. E-mail: luhuang@osdp.cs.tsukuba.ac.jp.*
- *J. Li (corresponding author) is with the Faculty of Engineering, Information and Systems, University of Tsukuba, Tsukuba, Japan. E-mail: lijie@cs.tsukuba.ac.jp.*
- *M. Guizani is with Qatar University, Doha, Qatar. E-mail: mguizani@ieee.org.*

distant CH.

The feasibility of the asymmetric key management has been shown in WSNs recently, which compensates the shortage from applying the symmetric key management for security [12]. Digital signature is one of the most critical security services offered by cryptography in asymmetric key management systems, where the binding between the public key and the identification of the signer is obtained via a digital certificate [13]. The Identity-Based digital Signature (IBS) scheme [14], based on the difficulty of factoring integers from Identity-Based Cryptography (IBC), is to derive an entity's public key from its identity information, e.g., from its name or ID number. Recently, the concept of IBS has been developed as a key management in WSNs for security. Carman [15] first combined the benefits of IBS and key pre-distribution set into WSNs, and some papers appeared in recent years [16–18]. The IBOOS scheme has been proposed in order to reduce the computation and storage costs of signature processing. A general method for constructing online/offline signature schemes was introduced by Even *et al.* [19]. The IBOOS scheme could be effective for the key management in WSNs. Specifically, the offline phase can be executed on a sensor node or at the BS prior to communication, while the online phase is to be executed during communication. Some IBOOS schemes are designed for WSNs afterwards, such as [20] and [21]. The offline signature in these schemes, however, is precomputed by a third party and lacks reusability, thus they are not suitable for CWSNs.

1.2 Contributions and Organization

Recently, we have applied and evaluated the key management of IBS to routing in CWSNs [17]. In this paper, we extend our previous work and focus on providing efficient secure data communication for CWSNs. The contributions of this work are as follows.

- We propose two **S**ecure and **E**fficient data **T**ransmission (SET) protocols for CWSNs, called **SET-IBS** and **SET-IBOOS**, by using the **IBS** scheme and the **IBOOS** scheme, respectively. The key idea of both SET-IBS and SET-IBOOS is to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security. In the proposed protocols, secret keys and pairing parameters are distributed and preloaded in all sensor nodes by the BS initially, which overcomes the key escrow problem described in ID-based crypto-systems [22].
- Secure communication in SET-IBS relies on the ID-based cryptography, in which, user public keys are their ID information. Thus, users can obtain the corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy.
- SET-IBOOS is proposed in order to further reduce the computational overhead for security using the IBOOS scheme, in which security relies on the hardness of the discrete logarithmic problem. Both SET-IBS and SET-IBOOS solve the orphan node problem in the secure data transmission with a symmetric key management.
- We show the feasibility of the proposed protocols with respect to the security requirements and analysis against three attack models. Moreover, we compare the proposed protocols with the existing secure protocols for efficiency by calculations and simulations respectively, with respect to both computation and communication.

The remainder of this paper is organized as follows. Section 2 describes the network architecture, security vulnerabilities and objectives. Section 3 introduces the IBS and IBOOS schemes for CWSNs. Section 4 and 5 present the details of the proposed SET-IBS and SET-IBOOS, respectively, and Section 6 presents the protocol features and characteristics. Section 7 analyzes and evaluates the proposed SET-IBS and SET-IBOOS. The last section concludes this work.

2 S D P O

This section presents the network architecture, security vulnerabilities and protocol objectives.

2.1 Network Architecture

Consider a CWSN consisting of a fixed base station (BS) and a large number of wireless sensor nodes, which are homogeneous in functionalities and capabilities. We assume that the BS is always reliable, i.e., the BS is a trusted authority (TA). Meanwhile, the sensor nodes may be compromised by attackers, and the data transmission may be interrupted from attacks on wireless channel. In a CWSN, sensor nodes are grouped into clusters, and each cluster has a cluster-head (CH) sensor node, which is elected autonomously. Leaf (non-CH) sensor nodes, join a cluster depending on the receiving signal strength and transmit the sensed data to the BS via CHs to save energy. The CHs perform data fusion, and transmit data to the BS directly with comparatively high energy. In addition, we assume that, all sensor nodes and the BS are time synchronized with symmetric radio channels, nodes are distributed randomly, and their energy is constrained.

In CWSNs, data sensing, processing and transmission consume energy of sensor nodes. The cost of data transmission is much more expensive than that of data processing. Thus, the method that the intermediate node (e.g., a CH) aggregates data and sends it to the BS is preferred, than the method that each sensor node directly sends data to the BS [1, 3]. A sensor node switches into sleep mode for energy saving when it does not sense or transmit data, depending on the TDMA (time division multiple access) control used for data transmission. In this paper, the proposed SET-IBS and SET-IBOOS are both designed for the same scenarios of CWSNs above.

2.2 Security Vulnerabilities and Protocol Objectives

The data transmission protocols for WSNs, including cluster-based protocols (LEACH-like protocols), are vulnerable to a number of security attacks [2, 23]. Especially, attacks to CHs in CWSNs could result in serious damage to the network, because data transmission and data aggregation depend on the CHs fundamentally. If an attacker manages to compromise or pretend to be a CH, it can provoke attacks such as sinkhole and selective forwarding attacks, hence disrupting the network.

On the other hand, an attacker may intend to inject bogus sensing data into the WSN, e.g., pretend as a leaf node sending bogus information towards the CHs. Nevertheless, LEACH-like protocols are more robust against insider attacks than other types of protocols in WSNs [23]. It is because CHs are rotating from nodes to nodes in the network by rounds, which makes it harder for intruders to identify the routing elements as the intermediary nodes and attack them. The characteristics of LEACH-like protocols reduce the risks of being attacked on intermediary nodes, and make it harder for an adversary to identify and compromise important nodes (CH nodes).

The goal of the proposed secure data transmission for CWSNs is to guarantee a secure and efficient data transmission between leaf nodes and CHs, as well as transmission between CHs and the BS. Meanwhile, most of existing secure transmission protocols for CWSNs in the literature [8–10], however, apply the symmetric key management for security, which suffers from the orphan node problem that is introduced in Section 1. In this paper, we aim to solve this orphan node problem by using the ID-based crypto-system that guarantees security requirements, and propose SET-IBS by using the IBS scheme. Furthermore, SET-IBOOS is proposed to reduce the computational overhead in SET-IBS with the IBOOS scheme.

3 IBS IBOOS CWSN

In this section, we introduce the IBS scheme and IBOOS scheme used in the paper. Note that the conventional schemes are not specifically designed for CWSNs. We adapt the conventional IBS scheme for CWSNs by distributing functions to different kinds of sensor nodes, based on [24] at first. In order to further reduce the computational overhead in the signing and verification process of the IBS scheme, we adapt the conventional IBOOS scheme for CWSNs, based on [21].

In a multiplicative finite cyclic group $\mathbb{G}$ of prime order q, there exists an element g as the generator and elements $g^x \in \mathbb{G}$, such that, $\mathbb{G} = \langle g \rangle = \left\{ g^x \mid x \in \mathbb{Z}_q^* = \{1, 2, \ldots, q-1\} \right\}$, where, $\mathbb{Z}_q^*$ is a multiplicative group consisting of q–1 integers, in which the multiplication operation in the group ends in the remainder on the division by q (mod q) [25]. The Discrete Logarithm Problem (DLP) [26] in the cyclic group $\mathbb{G}$ is to compute x, in which the computational complexity is believed to be hard, where the security in the IBOOS scheme is based on the DLP in this work.

3.1 Pairing for IBS

Boneh and Franklin [22] introduced the first functional and efficient ID-based encryption scheme based on bilinear pairings on elliptic curves. Specifically, randomly select two large primes p and q, and let $\mathbb{E}/\mathbb{F}_p$ indicate an elliptic curve $y^2 = x^3 + ax + b$ $(4a^3 + 27b^2 \neq 0)$ over a finite field $\mathbb{F}_p$. We denote by $\mathbb{G}_1$ a q-order subgroup of the additive group of points in $\mathbb{E}/\mathbb{F}_p$, and $\mathbb{G}_2$ a q-order subgroup of the multiplicative group in the finite field $\mathbb{F}_p^*$. The pairing is a mapping $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, which is a bilinear map with the following properties.

1) *Bilinear*: $\forall\ P, Q, R, S \in \mathbb{G}_1$, $e(P+Q, R+S) = e(P,R)\, e(P,S)\, e(Q,R)\, e(Q,S)$. In the same way, $\forall\ c, d \in \mathbb{Z}_q^*$, $e(cP, dQ) = e(P, dQ)^c = e(cP, Q)^d = e(P, Q)^{cd}$, etc.
2) *Non-degeneracy*: If P is a generator of $\mathbb{G}_1$, then $e(P, P)$ is a generator of $\mathbb{G}_2$.
3) *Computability*: There is an efficient algorithm to compute $e(P, Q)$ in $\mathbb{G}_2$, $\forall\ P, Q \in \mathbb{G}_1$.

The security in the IBS scheme is based on the bilinear Diffie-Hellman Problem (DHP) in the pairing domain [13], and the hardness of DHP is defined in [22]. A bilinear map e is secure if, given $g, G, H \in \mathbb{G}_1$, it is hard to find $h \in \mathbb{G}_1$ such that $e(h, H) = e(g, G)$ [27]. Weil pairing [22] and Tate pairing [28] are the examples of such bilinear mapping, which present comprehensive descriptions of how pairing parameters can be selected for security.

The notations used in the following are listed in Table I.

TABLE I: List of notations in IBS and IBOOS procedure

msk	master key
$param$	public parameters for the PKG
sek_{ID}	private key generated from an ID and the master key
t	time-stamp indicating the current time
θ	signing key used for signature signing and verification
SIG	digital signature generated from an IBS scheme
SIG_{offline}	offline digital signature generated from an IBOOS scheme
SIG_{online}	online digital signature generated using the SIG_{offline}

3.2 IBS Scheme for CWSNs

An IBS scheme implemented for CWSNs consists of the following operations, specifically, setup at the BS, key extraction and signature signing at the data sending nodes, and verification at the data receiving nodes.

- *Setup*: The BS (as a trust authority) generates a master key *msk* and public parameters *param* for the private key generator (PKG), and gives them to all sensor nodes.
- *Extraction*: Given an ID string, a sensor node generates a private key sek_{ID} associated with the ID using *msk*.
- *Signature signing*: Given a message M, time-stamp t and a signing key θ, the sending node generates a signature SIG.
- *Verification*: Given the ID, M and SIG, the receiving node outputs "accept" if SIG is valid, and outputs "reject" otherwise.

The detailed description of the original IBS scheme in [24] is given in Appendix A.[1]

3.3 IBOOS Scheme for CWSNs

An IBOOS scheme implemented for CWSNs consists of following four operations, specifically, setup at the BS, key extraction and offline signing at the CHs, online signing at the data sending nodes, and verification at the receiving nodes.

- *Setup*: Same as that in the IBS scheme.
- *Extraction*: Same as that in the IBS scheme.
- *Offline signing*: Given public parameters and time-stamp t, the CH sensor node generates an offline signature SIG_{offline}, and transmit it to the leaf nodes in its cluster.
- *Online signing*: From the private key sek_{ID}, SIG_{offline} and message M, a sending node (leaf node) generates an online signature SIG_{online}.

1. The appendices of this article are separated, which are available online: http://doi.ieeecomputersociety.org/10.1109/TPDS.2013.43.

• *Verification*: Given ID, M and SIG_{online}, the receiving node (CH node) outputs "accept" if SIG_{online} is valid, and outputs "reject" otherwise.

The detailed description of the original IBOOS scheme in [21] is given in Appendix B.[1]

4 T P SET-IBS P

In this paper, we propose two novel **S**ecure and **E**fficient data **T**ransmission (SET) protocols for CWSNs, called **SET-IBS** and **SET-IBOOS**, by using the **IBS** scheme and the **IBOOS** scheme, respectively. We first present SET-IBS in this section.

The proposed SET-IBS has a protocol initialization prior to the network deployment and operates in rounds during communication, which consists of a setup phase and a steady-state phase in each round. We introduce the protocol initialization, describe the key management of the protocol by using the IBS scheme, and the protocol operations afterwards.

4.1 Protocol initialization

In SET-IBS, time is divided into successive time intervals as other LEACH-like protocols. We denote time-stamps by T_s for BS-to-node communication and by t_j for leaf-to-CH communication. Note that key pre-distribution is an efficient method to improve communication security, which has been adapted in WSNs in the literature [8–10, 15–18, 29]. In this paper, we adopt $ID||t$ as user's public key under an IBS scheme [24], and propose a novel secure data transmission protocol by using IBS specifically for CWSNs (SET-IBS). The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. In this way, when a sensor node wants to authenticate itself to another node, it does not have to obtain its private key at the beginning of a new round. Upon node revocation, the BS broadcasts the compromised node IDs to all sensor nodes, each node then stores the revoked IDs within the current round. We adopt the additively homomorphic encryption scheme in [30] to encrypt the plaintext of sensed data, in which a specific operation performed on the plaintext is equivalent to the operation performed on the ciphertext. Using this scheme allows efficient aggregation of encrypted data at the CHs and the BS, which also guarantees data confidentiality. In the protocol initialization, the BS performs the following operations of key pre-distribution to all the sensor nodes.

- Generate an encryption key k for the homomorphic encryption scheme to encrypt data messages, where $k \in [m-1]$, m is a large integer.
- Generate the pairing parameters $(p, q, \mathbb{E}/\mathbb{F}_p, \mathbb{G}_1, \mathbb{G}_2, e)$, as described in Section 3. Select a generator P of $\mathbb{G}_1$ stochastically.
- Choose two cryptographic hash functions: H, for point mapping hash function which maps strings to elements in $\mathbb{G}_1$, and h, for mapping arbitrary inputs to fixed-length outputs.
- Pick a random integer $\tau \in \mathbb{Z}_q^*$ as the master key msk, set $P_{pub} = \tau P$ as network public key.
- Preload each sensor node with the system parameters $param = (k, m, p, q, \mathbb{E}/\mathbb{F}_p, \mathbb{G}_1, \mathbb{G}_2, e, H, h, P, \tau)$.

4.2 Key management for security

Assume that a leaf sensor node j transmits a message M to its CH i, and encrypts the data using the encryption key k from the additively homomorphic encryption scheme [30]. We denote the ciphertext of the encrypted message as C. We adapt the algorithms of the IBS scheme from [24] to CWSNs practically and provide the full algorithm in the signature verification, where security is based on the DHP in the multiplicative group. The IBS scheme in the proposed SET-IBS consists of following three operations, extraction, signing and verification.

Extraction: Node j first obtains its private key as $sek_j = \tau H(ID_j||t_j)$ from msk and ID_j, where ID_j is its ID, and t_j is the time-stamp of node j's time interval in the current round that is generated by its CH i from the TDMA (time division multiple access) control.

Signature signing: The sensor node j picks a random number $\alpha_j \in \mathbb{Z}_q^*$ and computes $\theta_j = e(P, P)^{\alpha_j}$. The sensor node further computes

$$c_j = h(C_j \| t_j \| \theta_j) . \tag{1}$$

Let

$$\sigma_j = c_j sek_j + \alpha_j P , \tag{2}$$

where $\langle \sigma_j, c_j \rangle$ is the digital signature of node j on the encrypted message C_j. The broadcast message is now concatenated in the form of $\langle ID_j, t_j, C_j, \sigma_j, c_j \rangle$.

Verification: Upon receiving the message, each sensor node verifies the authenticity in the following way. It checks the time-stamp of current time interval t_j and determines whether the received message is fresh. Then, if the time-stamp is correct, the sensor node further computes,

$$\theta'_j = e\left(\sigma_j, P\right) e\left(H(ID_j \| t_j), -P_{pub}\right)^{c_j} , \tag{3}$$

using the time-stamp of current time interval t_j. We will have the formula below if the received message is authentic.

$$\begin{aligned}
\theta'_j &= e\left(\sigma_j, P\right) e\left(H(ID_j \| t_j), -P_{pub}\right)^{c_j} \\
&= e\left(\sigma_j, P\right) e\left(H(ID_j \| t_j), -\tau P\right)^{c_j} \\
&= e\left(c_j sek_j + \alpha_j P, P\right) e\left(H(ID_j \| t_j), \tau P\right)^{-c_j} \\
&= e\left(c_j sek_j + \alpha_j P, P\right) e\left(\tau H(ID_j \| t_j), P\right)^{-c_j} \\
&= \left(e(sek_j, P)^{c_j} e(P, P)^{\alpha_j}\right) e\left(\tau H(ID_j \| t_j), P\right)^{-c_j} \\
&= e(sek_j, P)^{c_j} e(P, P)^{\alpha_j} e(sek_j, P)^{-c_j} \\
&= e(P, P)^{\alpha_j} = \theta_j .
\end{aligned} \tag{4}$$

If $h\left(C_j \| t_j \| \theta'_j\right) = h\left(C_j \| t_j \| \theta_j\right) = c_j$, which is equal to that in the received message, the sensor node considers the received message authentic, and propagates the message to the next hop or user. If the verification above fails, the sensor node considers the message as either bogus or a replaced one, even a mistaken one, and ignores it.

4.3 Protocol operation

After the protocol initialization, SET-IBS operates in rounds during communication. Each round consists of a setup phase and a steady-state phase. We suppose that, all sensor nodes

TABLE II: Operations in SET-IBS

Setup phase				
Step 1.	$BS \Rightarrow G_s$	:	$\langle ID_{bs}, T_s, nonce\rangle$	/* The BS broadcasts its information to all nodes. */
Step 2.	$CH_i \Rightarrow G_s$	:	$\langle ID_i, T_s, adv, \sigma_i, c_i\rangle$	/* The elected CHs broadcast their information. */
Step 3.	$L_j \rightarrow CH_i$	:	$\langle ID_i, ID_j, T_s, join, \sigma_j, c_j\rangle$	/* A leaf node joins a cluster of the CH i. */
Step 4.	$CH_i \Rightarrow G_s$	:	$\langle ID_i, T_s, sched(\ldots, ID_j/t_j, \ldots), \sigma_i, c_i\rangle$	/* A CH i broadcasts the schedule message to its members. */
Steady-state phase				
Step 5.	$L_j \rightarrow CH_i$	:	$\langle ID_i, ID_j, t_j, C_j, \sigma_j, c_j\rangle$	/* A leaf node j transmits the sensed data to its CH i. */
Step 6.	$CH_i \rightarrow BS$	:	$\langle ID_{bs}, ID_i, T_s, F_i, \sigma_i, c_i\rangle$	/* A CH i transmits the aggregated data to the BS. */

- ***Notations*** -	$\Rightarrow, \rightarrow$	:	Broadcast and unicast transmission.
	L_j, CH_i, G_s	:	A leaf node, a cluster head, and the set of sensor nodes in the network.
	T_s, t_j	:	Time-stamps denoting the time slot for transmission in setup and steady-state phases.
	ID_i, ID_{bs}	:	The IDs of a sensor node i and the BS.
	C_j, F_i	:	The encrypted sensed data of node j and the aggregated data of CH i.
	adv,join,sched	:	Message string types which denote the advertisement, join_request, and schedule messages.
	$\langle \sigma_i, c_i\rangle$	:	The ID-based digital signature concatenated with data from node i.

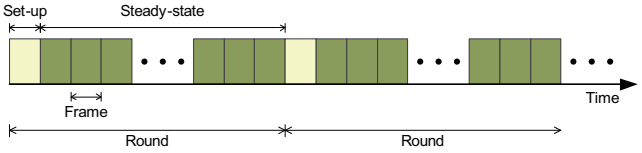

Fig. 1. Operation in the proposed secure data transmission

know the starting and ending time of each round, because of the time synchronization.

The operation of SET-IBS is divided by rounds as shown in Figure 1, which is similar to other LEACH-like protocols. Each round includes a setup phase for constructing clusters from CHs, and a steady-state phase for transmitting data from sensor nodes to the BS. In each round, the timeline is divided into consecutive time slots by the TDMA (time division multiple access) control [4]. Sensor nodes transmit the sensed data to the CHs in each frame of the steady-state phase. For fair energy consumption, nodes are randomly elected as CHs in each round, and other non-CH sensor nodes join clusters using one-hop transmission, depending on the highest received signal strength of CHs. In order to elect CHs in a new round, each sensor node determines a random number and compares it with a threshold. If the value is less than the threshold, the sensor node becomes a CH for the current round. In this way, the new CHs are self-elected based by the sensor nodes themselves only on their local decisions, therefore, SET-IBS functions without data transmission with each other in the CH rotations.

Table II shows the full steps in one round of SET-IBS. The setup phase consists of four steps, from Step 1 to 4, and the steady-state phase consists of the latter two steps. In the setup phase, the time-stamp T_s and node IDs are used for the signature generation. Whereas, in the steady-state phase, the time-stamp t_j is used for the signature generation securing the inner cluster communications, and T_s is used for the signature generation securing the CHs-to-BS data transmission.

In Step 1, at the beginning of the setup phase of a new round, the BS first broadcasts its ID, a *nonce* (number used once), and the denotation of the starting time T_s of the current round to all sensor nodes, which is used for the signature signing and verification in the setup phase.

In Step 2, a sensor node decides whether to become a CH for the current round, based on the threshold $T(n)$ compared with numbers from 0 to 1, which is set as follows:

$$T(n) = \begin{cases} \dfrac{\rho}{1-\rho\times\left(r \bmod \left\lfloor \frac{1}{\rho}\right\rfloor\right)} \cdot \dfrac{E_{cur}(n)}{E_{init}(n)} & \forall n \in G_n, \\ T(n) = 0 & \forall n \notin G_n. \end{cases} \quad (5)$$

Equation (5) of computing the threshold $T(n)$ in node n is based on the LEACH protocol [4]. Note that we improve the dynamic clustering algorithm preferably with multiplying the ratio of residual energy of the current sensor node (i.e., $\frac{E_{cur}(n)}{E_{init}(n)}$) to increase the energy efficiency in the clustering, where, $E_{cur}(n)$ is the current energy, and $E_{init}(n)$ is the initial energy of the sensor node. ρ is a priori determined value which stands for the desired percentage of CHs during one round (e.g., $\rho = 10\%$), r is the current round number, and G_n is the set of sensor nodes that have not been CHs in the last $\lfloor 1/\rho \rfloor$ rounds. If the value of determined number is less than the threshold, the sensor node elects itself as a CH. The sensor node who decides to become a CH broadcasts the advertisement message (*adv*) to the neighboring nodes in the network, which is concatenated with the signature $\langle \sigma_i, c_i\rangle$.

In Step 3, the sensor node, which decides to be a leaf node, picks a CH to join based on the largest received signal strength of *adv* messages. Then, it communicates with CH i by sending a join_request (*join*) message, which is concatenated with the destination CH's ID ID_i, its own ID ID_j, time-stamp T_s, and the digital signature $\langle \sigma_j, c_j\rangle$.

In Step 4, a CH i broadcasts an allocation message to its cluster members for communication during the steady-state phase, yet to be concatenated with the signature. The allocation message include a time schedule $\langle sched(\ldots, ID_j/t_j, \ldots)\rangle$ from the TDMA control, which allocates a time-stamp ID_j/t_j for a leaf node j.

Once the setup phase is over, the network system turns into the steady-state phase, in which sensed data is transmitted

from sensor nodes to the BS. In Step 5, according to the TDMA schedule from Step 4, each leaf sensor node j transmits the encrypted data C_j in a packet $\langle ID_j, t_j, C_j, \sigma_j, c_j\rangle$ to its CH, which is concatenated with a digital signature in a time slot t_j, where the sender ID ID_j with t_j is the destination identifier for the receiver CH. In this way, each CH collects messages from all members in its cluster, aggregates and fuses data.

In Step 6, CHs send the aggregated data F to the BS, yet to be concatenated with the digital signature. The steady-state phase consists of multiple reporting cycles of data transmissions from leaf nodes to the CHs, and is exceedingly long compared to the setup phase.

5 T P SET-IBOOS P

We present the **S**ecure and **E**fficient data **T**ransmission (SET) protocol for CWSNs by using IBOOS (SET-IBOOS) in this section. The SET-IBOOS protocol is designed with the same purpose and scenarios for CWSNs with higher efficiency. The proposed SET-IBOOS operates similarly to the previous SET-IBS, which has a protocol initialization prior to the network deployment and operates in rounds during communication. We first introduce the protocol initialization, then describe the key management of the protocol by using the IBOOS scheme, and the protocol operations afterwards.

5.1 Protocol initialization

In order to reduce the computation and storage costs of signature signing processing in the IBS scheme, we improve SET-IBS by introducing IBOOS for security in SET-IBOOS. The operation of the protocol initialization in SET-IBOOS is similar to that of SET-IBS, however, the operations of key pre-distribution are revised for IBOOS. The BS does the following operations of key pre-distribution in the network:

- Generate an encryption key k for the homomorphic encryption scheme to encrypt data messages, where $k \in [m-1]$, m is a large integer.
- Let $\mathbb{G}$ be a multiplicative finite cyclic group with order q. The PKG selects a random generator g of group $\mathbb{G}$ generation, and chooses $\tau \in \mathbb{Z}_q^*$ at random as the master key msk.
- For each node j, randomly select $r_j \in \mathbb{Z}_q^*$ for its private key generation, and let H be a hash function.
- Preload each sensor node j with the public parameters, given by $param_j = (k, m, \mathbb{G}, q, g, \tau, r_j, H)$.

5.2 Key management for security

Assume that a leaf sensor node j transmits a message M to its CH i, and we denote the ciphertext of the encrypted message as C_j, which is encrypted by the same encryption scheme in SET-IBS. We adapt the algorithms from [21] to construct an IBOOS scheme for CWSNs, where security is based on the DLP in the multiplicative group. The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. The IBOOS scheme in the proposed SET-IBOOS consists of following four operations, extraction, offline signing, online signing and verification.

Extraction: Before the signature process, node j first extracts the private key from the msk τ and its identity ID, as $sek_j = (R_j, s_j)$, where

$$\begin{aligned} R_j &= g^{r_j}, \\ s_j &= r_j + H(R_j, ID_j)\tau \bmod q. \end{aligned} \tag{6}$$

Offline signing: At the offline stage, node j generates the offline value $\langle \widehat{\sigma}_j \rangle$ with the time-stamp of its time slot t_j for transmission, and store the knowledge for signing online signature when it sends the message. Notice that, this offline signature can be done by the sensor node itself or by the trustful third party, e.g., the CH sensor node. Let $X = g^{\tau}$, then,

$$\begin{aligned} g^{s_j} &= g^{r_j} g^{H(R_j, ID_j)\tau \bmod q} = R_j X^{H(R_j, ID_j) \bmod q}. \\ \widehat{\sigma}_j &= g^{-t_j}. \end{aligned} \tag{7}$$

Online signing: At this stage, node j computes the online signature $\langle \sigma_j, z_j \rangle$ based on the encrypted data C_j and the offline signature $\widehat{\sigma}_j$.

$$\begin{aligned} h_j &= H(C_j \| ID_i). \\ z_j &= \widehat{\sigma}_j + h_j s_j \bmod q, \\ \sigma_j &= g^{\widehat{\sigma_j}}. \end{aligned} \tag{8}$$

Then node j sends the message to its destination with t_j, R_j and the online signature, in the form of $\langle ID_j, t_j, R_j, \sigma_j, z_j, C_j \rangle$.

Verification: Upon receiving the message, each sensor node verifies the authenticity in the following way. It checks the current time-stamp t_j for freshness. Then, if the time-stamp is correct, the sensor node further computes the values of g^{z_j} and $\sigma_j R_j^{h_j} X^{h_j H(R_j, ID_j) \bmod q}$, then check if

$$g^{z_j} \stackrel{?}{=} \sigma_j R_j^{h_j} X^{h_j H(R_j, ID_j) \bmod q}. \tag{9}$$

For correctness, we will have the formula below if the received message is authentic.

$$\begin{aligned} &\sigma_j R^{h_j} X^{h_j H(R_j, ID_j) \bmod q} \\ &= g^{\widehat{\sigma}_j} g^{r_j h_j} g^{\tau h_i H(R_j, ID_j) \bmod q} \\ &= g^{\widehat{\sigma}_j + h_j (r_j + (H(R_j, ID_j)\tau \bmod q))} \\ &= g^{\widehat{\sigma}_j + h_j s_j \bmod q} = g^{z_j}. \end{aligned} \tag{10}$$

If the value of g^{z_j} and $\sigma_j R_i^{h_i} X^{h_i H(R_i, ID_i) \bmod q}$ are equal from the received message, the node i considers the received message authentic, accepts it, and propagates the message to the next hop or user. If the verification above fails, the sensor node considers the message as either bogus or a replaced one, even a mistaken one, then rejects or ignores it.

5.3 Protocol operation

The proposed SET-IBOOS operates similarly to that of SET-IBS. SET-IBOOS works in rounds during communication, and the self-elected CHs are decided based on their local decisions, thus it functions without data transmission in the CH rotations. Table III shows the full steps of SET-IBOOS in one round, in which the setup phase is from Step 1 to 4, and the steady-state phase consists of Step 5 and 6.

Step 1 in Table III is similar to that in Table II. However, the differences in Steps 2, 3 and 4 are the digital signatures

TABLE III: Operations in SET-IBOOS

Setup phase				
Step 1.	$BS \Rightarrow G_s$	:	$\langle ID_{bs}, T_s, nonce\rangle$	/* The BS broadcasts its information to all nodes. */
Step 2.	$CH_i \Rightarrow G_s$	:	$\langle ID_i, T_s, adv, R_i, \sigma_i, z_i\rangle$	/* The elected CHs broadcast their information. */
Step 3.	$L_j \rightarrow CH_i$	:	$\langle ID_i, ID_j, T_s, join, R_j, \sigma_j, z_j\rangle$	/* A leaf node joins a cluster of CH i. */
Step 4.	$CH_i \Rightarrow G_s$	:	$\langle ID_i, T_s, alloc(\ldots, ID_j/t_j, \ldots), R_i, \sigma_i, z_i\rangle$	/* A CH i broadcasts the allocation message. */
Steady-state phase				
Step 5.	$L_j \rightarrow CH_i$	:	$\langle ID_i, ID_j, t_j, C_j, R_j, \sigma_j, z_j\rangle$	/* A leaf node j transmits the sensed data to its CH i. */
Step 6.	$CH_i \rightarrow BS$	:	$\langle ID_{bs}, ID_i, T_s, F_i, R_i, \sigma_i, z_i\rangle$	/* A CH i transmits the aggregated data to the BS. */

- ***Notations*** -	$\Rightarrow, \rightarrow$	:	Broadcast and unicast transmission.
	L_j, CH_i, G_s	:	A leaf node, a cluster head, and the set of sensor nodes in the network.
	T_s, t_j	:	Time-stamps denoting the time slot for transmission in setup and steady-state phases.
	ID_i, ID_{bs}	:	The IDs of a sensor node i and the BS.
	C_j, F_i	:	The encrypted sensed data of node j and the aggregated data of CH i.
	$adv, join, alloc$	:	Message string types which denote the advertisement, join_request, and allocation messages.
	$\langle R_i, \sigma_i, z_i\rangle$	:	The online signature of node i concatenated with data.

which are changed from the ID-based signatures to the online signatures $\langle \sigma_i, z_i\rangle$ of the IBOOS scheme.

Once the setup phase is over, the network system turns into the steady-state phase, in which data is transmitted to the BS. The steady-state operates similarly to that in steps 5 and 6 of Table II, where the ID-based signatures are changed into the online signatures of the IBOOS scheme.

For convenience, we show a flowchart of the proposed secure data transmission protocols in Appendix C.[1]

6 P F

The protocol characteristics and hierarchical clustering solutions are presented in this section. We first summarize the features of the proposed SET-IBS and SET-IBOOS protocols as follows.

- Both the proposed SET-IBS and SET-IBOOS protocols provide secure data transmission for CWSNs with concrete ID-based settings, which use ID information and digital signature for authentication. Thus, both SET-IBS and SET-IBOOS fully solve the orphan-node problem from using the symmetric key management for CWSNs.
- The proposed secure data transmission protocols are with concrete ID-based settings, which use ID information and digital signature for verification. Comparing the SET-IBS, SET-IBOOS requires less energy for computation and storage. Moreover, the SET-IBOOS is more suitable for node-to-node communications in CWSNs, since the computation is lighter to be executed.
- In SET-IBOOS, the offline signature is executed by the CH sensor nodes, thus, sensor nodes do not have to execute the offline algorithm before it wants to sign on a new message. Furthermore, the offline sign phase does not use any sensed data or secret information for signing. This is particularly useful for CWSNs, because leaf sensor nodes do not need auxiliary communication for renewing the offline signature.

6.1 Protocol Characteristics

In this part, we summarize the characteristics of the proposed SET-IBS and SET-IBOOS protocols. Table IV shows a general summary of comparison of the characteristics of SET-IBS and SET-IBOOS with prior ones, in which metrics are used to evaluate whether a security protocol is appropriate for CWSNs. We explain each metric as follows.

TABLE IV: Comparison of characteristics of the proposed protocols with other secure data transmission protocols

	SET-IBS / SET-IBOOS	Prior protocols [8–10]
Key management	Asymmetric	Symmetric
Neighborhood authentication	Yes	Limited
Storage cost	Comparative low	Comparative high
Network scalability	Comparative high	Comparative low
Communication overhead	Deterministic	Probabilistic
computational overhead	Comparative high	Low ~ high
Attack resilience	Passive and active attacks on wireless channel	

- *Key management*: the key cryptographies used in the protocol to achieve secure data transmission, which consist of symmetric and asymmetric key based security.
- *Neighborhood authentication*: used for secure access and data transmission to nearby sensor nodes, by authenticating with each other. Here, "limited" means the probability of neighborhood authentication, where only the nodes with the shared pairwise key can authenticate each other.
- *Storage cost*: represents the requirement of the security keys stored in sensor node's memory.
- *Network scalability*: indicates whether a security protocol is able to scale without compromising the security requirements. Here, "comparative low" means that, compared with SET-IBS and SET-IBOOS, in the secure data transmission with a symmetric key management, the larger network scale

increases, the more orphan nodes appear in the network, and vice versa [2].

- *Communication overhead*: the security overhead in the data packets during communication.
- *Computational overhead*: the energy cost and computation efficiency on the generation and verification of the certificates or signatures for security.
- *Attack resilience*: the types of attacks that security protocol can protect against.

6.2 Secure Data Transmission with Hierarchical Clustering

In large scale CWSNs, multi-hop data transmission is used for transmission between the CHs to the BS, where the direct communication is not possible due to the distance or obstacles between them. The version of the proposed SET-IBS and SET-IBOOS protocols for CWSNs can be extended using multi-hop routing algorithms, to form secure data transmission protocols for hierarchical clusters. The solutions to this extension could be achieved by applying the following two routing models.

1) The multi-hop planar model: A CH node transmits data to the BS by forwarding its data to its neighbor nodes, in turn the data is sent to the BS. We have proposed an energy efficient routing algorithm for hierarchically clustered WSNs in [31], and it is suitable for the proposed secure data transmission protocols.
2) The cluster-based hierarchical method: The network is broken into clustered layers, and the data packages travel from a lower cluster head to a higher one, in turn to the BS, e.g., [32].

7 P E

In this section, we first introduce the three attack models of the adversaries, and provide the security analysis of the proposed protocols against these attacks. We then present results obtained from calculations and simulations. For the network simulations, we use the network simulator OMNeT++ 3.0 [33] to simulate SET-IBS and SET-IBOOS, and we focus on the energy consumption spent on message propagation and computation.

7.1 Security Analysis

In order to evaluate the security of the proposed protocols, we have to investigate the attack models in WSNs which threaten the proposed protocols, and the cases when an adversary (attacker) exists in the network. Afterwards, we detail the solutions and countermeasures of the proposed protocols, against various adversaries and attacks.

7.1.1 Attack Models

In this paper, we group attack models into three categories according to their attacking means as follows, and study how these attacks may be applied to affect the proposed protocols.

- *Passive attack on wireless channel*: Passive attackers are able to perform eavesdropping at any point of the network, or even the whole communication of the network. Thus, they can undertake traffic analysis or statistical analysis based on the monitored or eavesdropped messages.
- *Active attack on wireless channel*: Active attackers have greater ability than passive adversaries, which can tamper with the wireless channels. Therefore, the attackers can forge, reply and modify messages. Especially in WSNs, various types of active attacks can be triggered by attackers, such as bogus and replayed routing information attack, sinkhole and wormhole attack, selective forwarding attack, HELLO flood attack, and Sybil attack [2, 23].
- *Node compromising attack*: Node compromising Attackers are the most powerful adversaries against the proposed protocols as we considered. The attackers can physically compromise sensor nodes, by which they can access the secret information stored in the compromised nodes, e.g., the security keys. The attackers also can change the inner state and behavior of the compromised sensor node, whose actions may be varied from the premier protocol specifications.

7.1.2 Solutions to Attacks and Adversaries

The proposed SET-IBS and SET-IBOOS provide different types of security services to the communication for CWSNs, in both setup phase and steady-state phase. Both in SET-IBS and SET-IBOOS, the encryption of the message provides confidentiality, the hash function provides integrity, the nonce and time-stamps provide freshness, and the digital signature provides authenticity and non-repudiation.

- *Solutions to passive attacks on wireless channel*: In the proposed SET-IBS and SET-IBOOS, the sensed data is encrypted by the homomorphic encryption scheme from [30], which deals with eavesdropping. Thus, the passive adversaries cannot decrypt the eavesdropped message without the decryption key. Furthermore, both SET-IBS and SET-IBOOS use the key management of concrete ID-based encryption. Based on the DHP assumption mentioned in Section 3, the ID-based key management in the proposed protocols is IND-ID-CCA secure (semantic secure against an adaptive ID-based chosen ciphertext attack) and IND-ID-CPA secure (semantic secure against an adaptive ID-based chosen plaintext attack). As a result, properties of the proposed secure data transmission for CWSNs settle the countermeasures to passive attacks.
- *Solutions to active attacks on wireless channel*: Focusing on the resilience against certain attacks to CWSNs mentioned in attack models, SET-IBS and SET-IBOOS work well against active attacks. Most kinds of attacks are pointed to CHs of acting as intermediary nodes, because of the limited functions by the leaf nodes in a cluster-based architecture. Since attackers do not have valid digital signature to concatenate with broadcast messages for authentication, attackers cannot pretend as the BS or CHs to trigger attacks. Therefore, SET-IBS and SET-IBOOS are resilient, and robust to the sinkhole and selective forwarding attacks, because the CHs being attacked are capable to ignore all the communication packets with bogus node IDs or bogus digital signatures. Together with round-rotating mechanism and digital signature schemes, SET-IBS and SET-IBOOS are resilient to the hello flood attacks involving CHs.

• *Solutions to node compromising attacks*: In case of attacks from a node compromising attacker, the compromised sensor node cannot be trusted anymore to fulfil the security requirements by key managements. In the case that the node has been compromised but works normally, the WSN system needs an intrusion detection mechanism to detect the compromised node [34], and has to replace the compromised node manually or abandon using it. In this part, we investigate the influence of the remaining sensor nodes, and evaluate the properties only to that part of the network.

Since each round in the protocol operations terminates in a pre-defined time, SET-IBS and SET-IBOOS satisfy the property of protocol execution termination, depending on the local timer of the sensor nodes. The CH nodes are elected based only on their local decisions, therefore, both SET-IBS and SET-IBOOS operate if there exists an active or compromising attacker. In order to eliminate the compromised sensor node in the network, all the revoked IDs of compromised nodes will be broadcast by the BS at the beginning of the current round. In this way, the compromised nodes can be prevented from either electing as CHs or joining clusters in this round. Furthermore, using either the IBS scheme or the IBOOS scheme has at least two advantages. First, it eliminates the utilization of certificates and auxiliary authentication information. Therefore, the message overhead for security can be reduced, especially with IBOOS. Also, because only the compromised node IDs have to be stored, it requires very small storage space for the node revocation. Since the length of a user's ID is usually only 1~2 *bytes*, the storage of compromised user's IDs do not require much storage space.

7.2 Message Size of Data Transmission

In this part, we do the quantitative calculation of the message packet size on data transmission in the steady-state (main phase) of the different protocols for comparison. In the proposed SET-IBS, the message packet size on transmission for node j is described in Section 4, which equals to

$$|ID_i| + |ID_j| + |t_j| + |C_j| + |\sigma_j| + |c_j|.$$

$c_j = |h(C_j||t_j||\theta_j)|$ is a hash value, which is 20 *bytes* when SHA-1 [35] is used. Although most of existing WSNs constructed in real world use no more than 200 nodes [1], a large scale WSN could consist of hundreds of nodes or more in the future. Thus in this paper, we set the length of node IDs as 2 *bytes*. In addition, the time-stamp $|t_j|$ is very small like 1 *byte*, and $|C_j|$ is assumed as 20 *bytes*. The total message size of a transmission packet is $44 + |\sigma_j|$ *bytes*, whereas, $|\sigma_j|$ is variable. For example, when using the Tate pairing [28] for elliptic curve cryptography (ECC), the order q of $\mathbb{G}_1$ and $\mathbb{G}_2$ could be a 160-bit prime, if the required security level of ECC is equivalent to RSA with 1024-bit keys (RSA-1024) [36], which provides the currently accepted security level. In this way, the total message size of a data packet is 64 *bytes* in SET-IBS. Moreover, p could be a 512-bit prime to achieve higher level of security, where $\mathbb{G}$ is a q-order multiplicative subgroup of the finite field $\mathbb{F}^*_{p^2}$ [22].

In SET-IBOOS, the message packet size on transmission for node j is described in Section 5, which equals to

$$|ID_i| + |ID_j| + |t_j| + |C_j| + |R_j| + |\sigma_j| + |z_j|.$$

the length of ID and t are same to that of SET-IBS, and $|C_j|$ is assumed as 20 *bytes*. In the online signature $\langle R_j, \sigma_j, z_j \rangle$, the length of $|z| = |\widehat{\sigma}_j + (hs \bmod q)|$ depends on the size of q, which is set to 160 bits long to achieve a similar security level of SET-IBS, because the offline signature $\widehat{\sigma}_j$ is a negative exponential value of the cyclic group $\mathbb{G}$'s generator g (in Equation 7) that is very small. For the other parts of the signature $\langle \sigma_j, z_j \rangle$, $|\sigma_j|$ is the exponentiation to the power $\widehat{\sigma}_j$, from the negative exponential function ($-t_j$, in Equation 8) of the generator g, thus its value is very small, which is assumed as 2 *bytes* at most in this paper. Similarly, the length of R_j is assumed as 2 *bytes*. Therefore, the total message size of a data packet is 48 *bytes* in SET-IBOOS.

We compare the proposed SET-IBS and SET-IBOOS with other secure protocols which use a symmetric key management, SecLEACH protocol[8] and multi-level μTesla based protocol [37]. We calculate the packet size in these protocols in the same way, which equals to

$$|ID_j| + |ID_{CH}| + |nonce| + |C_j| + |mac_k(ID_j|ID_{CH}|nonce|C_j)|,$$

in SecLEACH protocol, where *mac* is the message authentication code. And it equals to

$$|ID_j| + |t_j| + |C_j| + |Sig_{SK}\left\{h(ID_j|t_j|C_j)\right\}| + |PK| + |AI_j|,$$

in Multi-level μTesla based protocol, where *Sig* is the signature based on the secret key, *SK*/*PK* is the public/private key pair for signing and verification, and *AI* is the auxiliary information for security referred to the sensor node.

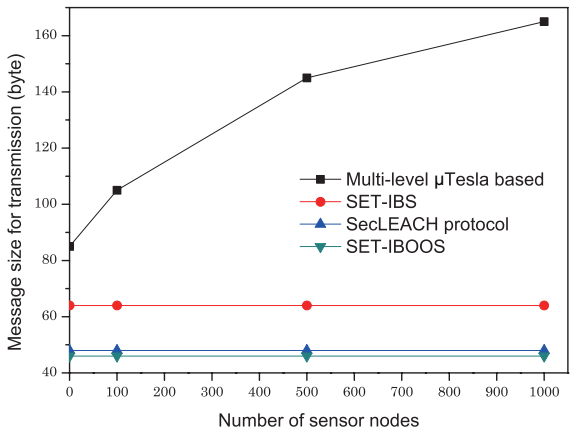

Fig. 2. Message size for transmission compared to the number of nodes

Figure 2 shows the total message sizes in different protocols for data transmission, which achieve a similar security level to RSA-1024, by concerning the number of sensor nodes. We can see that the proposed SET-IBS has smaller message size than multi-level μTesla based protocol. At the same time, it generates larger message size as compared to SecLEACH. However, the orphan node problem is fully solved in SET-IBS. We can also see that the proposed SET-IBOOS has the smallest message size than all the other protocols. We

further do network simulations on energy consumption and computation cost in the next subsection.

7.3 Simulation Results

Comprehending the extra energy consumption by the auxiliary security overhead and prolonging the network lifetime are essential in the proposed SET-IBS and SET-IBOOS. In order to evaluate the energy consumption of the computational overhead for security in communication, we consider three metrics for the performance evaluation: *Network lifetime*, *system energy consumption* and *the number of alive nodes*. For the performance evaluation, we compare the proposed SET-IBS and SET-IBOOS with LEACH protocol [4] and SecLEACH protocol [8].

- *Network lifetime* (the time of FND) - We use the most general metric in this paper, the time of FND (first node dies), which indicates the duration that the sensor network is fully functional [1]. Therefore, maximizing the time of FND in a WSN means to prolong the network lifetime.
- *The number of alive nodes* - The ability of sensing and collecting information in a WSN depends on the set of alive nodes (nodes that have not failed). Therefore, we evaluate the functionality of the WSN depending on counting the number of alive nodes in the network.
- *Total system energy consumption* - It refers to the amount of energy consumed in a WSN. We evaluate the variation of energy consumption in secure data transmission protocols.

In the network simulation experiments, 100 nodes are randomly distributed in a $100m \times 100m$ area, with a fixed BS located near part of the area, as shown in Figure 3. All the sensor nodes periodically sense events and transmit the data packet to the BS. We assume that the sensor CPU is a low-power high-performance Intel PXA255 processer of 400 MHz, which has been widely used in many sensor products, e.g., Crossbow Stargate [38].

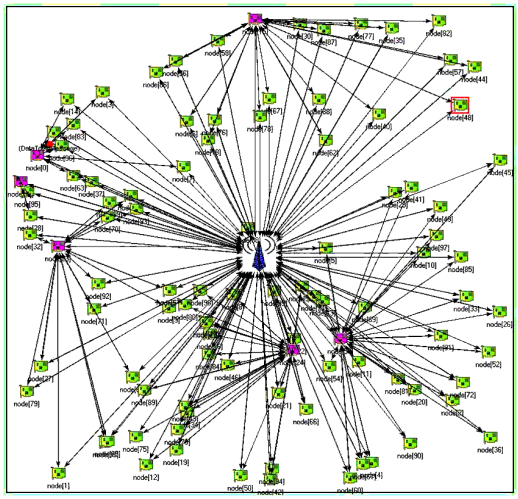

Fig. 3. An illustration of simulation topology for CWSNs

Table V lists up the parameter settings for the energy consumption in the network simulations. In the simulations, we use the same radio energy model in [4], and the other parameters are from [8, 21, 22, 24]. We assume that the BS has unlimited energy. For clustering, we properly set the desired

TABLE V: Parameter settings for the energy consumption in simulations

Node initial energy E_{init}	$1J$
Energy consumption on data aggregation E_{aggr}	$5nJ/bit$
Energy consumption on transmission amplifier E_{amp}	$100pJ/bit/m^2$
Energy consumption on signature signing and verification for SET-IBS E_{sig}	$77.4\mu J/signature$
Energy consumption on offline signature generation for SET-IBOOS $E_{offline}$	$5\mu J/signature$
Energy consumption on online signature signing and verification for SET-IBOOS E_{online}	$12.37\mu J/signature$
Hop-wise energy consumption on sending messages E_{send}	$59.2\mu J/byte$
Hop-wise energy consumption on receiving messages $E_{receive}$	$28.6\mu J/byte$

percentage of CH nodes $\rho = 10\%$ during one round. In addition, on simulating the SecLEACH protocol, we choose a security level $sl = 0.98$ for a fixed length of a key ring $m = 100$. Thus, the probability that two nodes will share a key is $P_s = 0.87$, which is also referred to as the expected orphan rate of the orphan node problem.

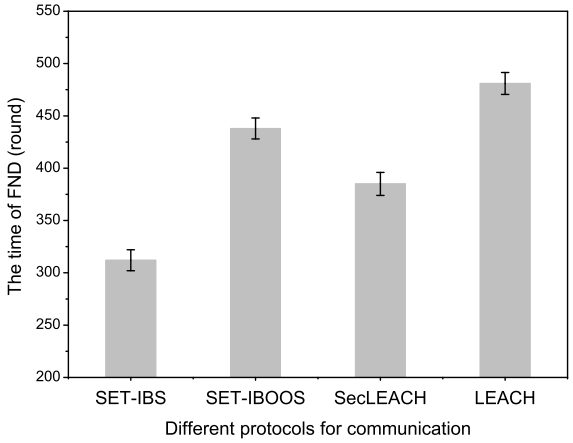

Fig. 4. Comparison of FND time in different protocols

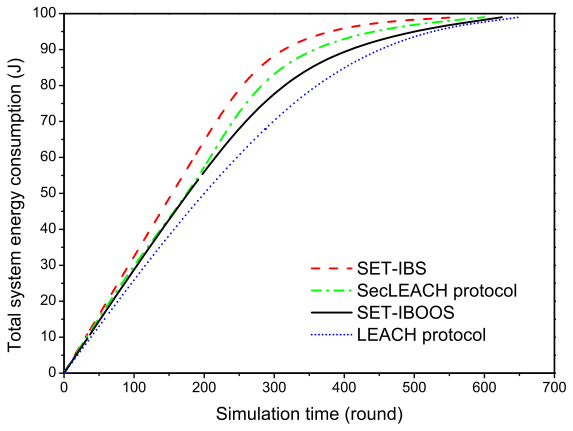

Fig. 5. Comparison of energy consumption in different protocols

Figure 4 illustrates the time of FND using different protocols. We apply confidence intervals to the simulation results, and a certain percentage (confidence level) is set to 90%. Figure 6 shows the comparison of system lifetime using SET-IBS and SET-IBOOS versus LEACH protocol and SecLEACH

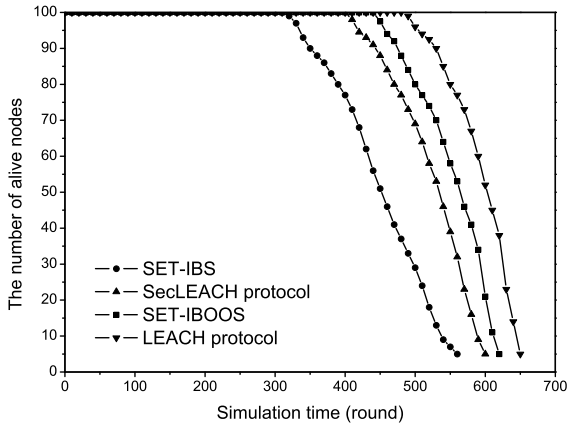

Fig. 6. Comparison of the number of alive nodes in different protocols

protocol. The simulation results demonstrate that the system lifetime of SET-IBOOS is longer than that of SET-IBS and SecLEACH protocol. The time of FND in both SET-IBS and SET-IBOOS is shorter than that of LEACH protocol due to the security overhead on computation cost of the IBS process.

Figure 5 illustrates the energy of all sensor nodes disseminated in the network, which also indicates the balance of energy consumption in the network. Figure 6 shows the comparison of alive nodes' number, in which the proposed SET-IBS and SET-IBOOS protocols versus LEACH and SecLEACH protocols. The results demonstrate that the proposed SET-IBS and SET-IBOOS protocols consume energy faster than LEACH protocol, because of the communication and computational overhead for security of either IBS or IBOOS process. However, the proposed SET-IBOOS has a better balance of energy consumption than that of SecLEACH protocol.

8 C

In this paper, we first reviewed the data transmission issues and the security issues in CWSNs. The deficiency of the symmetric key management for secure data transmission has been discussed. We then presented two secure and efficient data transmission protocols respectively for CWSNs, SET-IBS and SET-IBOOS. In the evaluation section, we provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks. SET-IBS and SET-IBOOS are efficient in communication and applying the ID-based crypto-system, which achieves security requirements in CWSNs, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management. Lastly, the comparison in the calculation and simulation results show that, the proposed SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for CWSNs. With respect to both computation and communication costs, we pointed out the merits that, using SET-IBOOS with less auxiliary security overhead is preferred for secure data transmission in CWSNs.

A

The authors would like to thank the Associate Editor and the anonymous reviewers, for their valuable suggestions and comments that improved this paper.

R

[1] T. Hara, V. I. Zadorozhny, and E. Buchmann, *Wireless Sensor Network Technologies for the Information Explosion Era, Stud. Comput. Intell.* Springer-Verlag, 2010, vol. 278.

[2] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," *IEEE Commun. Surveys Tuts.*, vol. 8, no. 2, pp. 2–23, 2006.

[3] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Comput. Commun.*, vol. 30, no. 14-15, pp. 2826–2841, 2007.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670, 2002.

[5] A. Manjeshwar, Q.-A.Zeng, and D. P. Agrawal, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," *IEEE Trans. Parallel Distrib. Syst.*, vol. 13, pp. 1290–1302, 2002.

[6] S. Yi, J. Heo, Y. Cho *et al.*, "PEACH: Power-efficient and adaptive clustering hierarchy protocol for wireless sensor networks," *Comput. Commun.*, vol. 30, no. 14-15, pp. 2842–2852, 2007.

[7] K. Pradeepa, W. R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," *Int. J. Comput. Applications*, vol. 47, no. 11, pp. 23–28, 2012.

[8] L. B. Oliveira, A. Ferreira, M. A. Vilaça *et al.*, "SecLEACH-On the security of clustered sensor networks," *Signal Process.*, vol. 87, pp. 2882–2895, 2007.

[9] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and performance analysis of a secure clustering protocol for sensor networks," in *Proc. IEEE NCA*, 2007, pp. 145–152.

[10] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," in *Proc. WiCOM*, 2008, pp. 1–5.

[11] S. Sharma and S. K. Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks," in *Proc. ICCCS*, 2011, pp. 146–151.

[12] G. Gaubatz, J. P. Kaps, E. Ozturk *et al.*, "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks," in *Proc. IEEE PerCom Workshops*, 2005, pp. 146–150.

[13] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[14] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in *Lect. Notes. Comput. Sc. - CRYPTO*, 1985, vol. 196, pp. 47–53.

[15] D. W. Carman, "New Directions in Sensor Network Key Management," *Int. J. Distrib. Sens. Netw.*, vol. 1, pp. 3–15, 2005.

[16] R. Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures," in *Proc. IEEE CIT*, 2010, pp. 882–889.

[17] H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID-Based Digital Signature," in *Proc. IEEE GLOBECOM*, 2010, pp. 1–5.

[18] J. Sun, C. Zhang, Y. Zhang *et al.*, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 9, pp. 1227–1239, 2010.

[19] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures," in *Lect. Notes. Comput. Sc. - CRYPTO*, 1990, vol. 435, pp. 263–275.

[20] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security," in *Lect. Notes. Comput. Sc. - Inf. Secur. Privacy*, 2006, vol. 4058, pp. 99–110.

[21] J. Liu, J. Baek, J. Zhou *et al.*, "Efficient online/offline identity-based signature for wireless sensor network," *Int. J. Inf. Secur.*, vol. 9, no. 4, pp. 287–296, 2010.

[22] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," in *Lect. Notes. Comput. Sc. - CRYPTO*, 2001, vol. 2139, pp. 213–229.

[23] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[24] F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," in *Lect. Notes. Comput. Sc. - SAC*, 2003, vol. 2595, pp. 310–324.

[25] J. J. Rotman, *An Introduction to the Theory of Groups*. Springer-Verlag; 4th edition, 1994.

[26] K. S. McCurley, "The Discrete Logarithm Problem," in *Proc. Symp. Appl. Math., Prog. Com. Sc.*, 1990, vol. 42, pp. 49–74.

[27] D. Boneh, I. Mironov, and V. Shoup, "A Secure Signature Scheme from

Bilinear Maps," in *Lect. Notes. Comput. Sc. - CT-RSA*, 2003, vol. 2612, pp. 98–110.
[28] P. Barreto, H. Kim, B. Lynn *et al.*, "Efficient Algorithms for Pairing-Based Cryptosystems," in *Lect. Notes. Comput. Sc. - CRYPTO*, 2002, vol. 2442, pp. 354–369.
[29] H. Lu, J. Li, and M. Guizani, "A Novel ID-based Authentication Framework with Adaptive Privacy Preservation for VANETs," in *Proc. ComComAp*, 2012, pp. 345–450.
[30] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor networks," in *Proc. MobiQuitous*, 2005, pp. 109–117.
[31] H. Lu, J. Li, and G. Wang, "A Novel Energy Efficient Routing Algorithm for Hierarchically Clustered Wireless Sensor Networks," in *Proc. FCST*, 2009, pp. 565–570.
[32] Y. Jia, L. Zhao, and B. Ma, "A Hierarchical Clustering-based Routing Protocol for Wireless Sensor Networks Supporting Multiple Data Aggregation Qualities," *IEEE Trans. Parallel Distrib. Syst.*, vol. 4, no. 1-2, pp. 79–91, 2008.
[33] "OMNeT++," OMNeT++ Community. URL: http://www.omnetpp.org/
[34] B. Sun, L. Osborne, Y. Xiao *et al.*, "Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks," *IEEE Wireless Commun. Mag.*, vol. 14, no. 5, pp. 56–63, 2007.
[35] *Secure Hash Standard*, National Institute of Standards and Technology (NIST), Fed. Inf. Process. Stand. Publ. 180-1, 1995.
[36] D. Hankerson, S. Vanstone, and A. Menezes, *Guide to Elliptic Curve Cryptography*, *Springer Prof. Comput.* Springer, 2004.
[37] D. Liu and P. Ning, "Multilevel μTESLA: Broadcast Authentication for Distributed Sensor Networks," *ACM Trans. Embed. Comput. Syst.*, vol. 3, pp. 800–836, 2004.
[38] "Crossbow Stargate," Crossbow Technology. URL: http://bullseye.xbow.com:81/Products/productdetails.aspx?sid=229

Huang Lu (S'10) studied in Harbin Institute of Technology, Harbin, China, before he went to Japan for overseas exchange. He received the B.S. degree in Information and Network Science from Chiba Institute of Technology, Chiba, Japan, and the M.S. degree in Computer Science from University of Tsukuba, Tsukuba, Japan, in 2007 and 2009, respectively. He is currently a Ph.D. candidate at Department of Computer Science, Graduate School of Systems and Information Engineering, University of Tsukuba, Tsukuba, Japan.

His research interests include wireless ad hoc and sensor networks, routing protocols, and network security. He is a student member of IEEE.

Jie Li (M'96-SM'04) received the B.E. degree in Computer Science from Zhejiang University, Hangzhou, China, the M.E. degree in Electronic Engineering and Communication Systems from China Academy of Posts and Telecommunications, Beijing, China. He received the Dr. Eng. degree from the University of Electro-Communications, Tokyo, Japan. He has been with University of Tsukuba, Tsukuba, Japan, where he is a Professor in Faculty of Engineering, Information and Systems.

His research interests are in mobile distributed multimedia computing and networking, OS, network security, modeling and performance evaluation of information systems. He received the best paper award from IEEE NAECON'97. He is a senior member of IEEE and ACM, and a member of IPSJ (Information Processing Society of Japan). He has served as a secretary for Study Group on System Evaluation of IPSJ and on several editorial boards for IPSJ Journal and so on, and on Steering Committees of the SIG of System EVAluation (EVA) of IPSJ, the SIG of DataBase System (DBS) of IPSJ, and the SIG of MoBiLe computing and ubiquitous communications (MBL) of IPSJ. He has been a co-chair of several international symposia and workshops. He has also served on the program committees for several international conferences such as IEEE ICDCS, IEEE INFOCOM, IEEE GLOBECOM, and IEEE MASS.

Mohsen Guizani (S'85-M'89-SM'99-F'09) is currently a Professor and the Associate Vice President for Graduate Studies at Qatar University, Doha, Qatar. He was the Chair of the Computer Science Department at Western Michigan University from 2002 to 2006 and Chair of the Computer Science Department at University of West Florida from 1999 to 2002. He also served in academic positions at the University of Missouri-Kansas City, University of Colorado-Boulder, Syracuse University and Kuwait University. He received his B.S. (with distinction) and M.S. degrees in Electrical Engineering; M.S. and Ph.D. degrees in Computer Engineering in 1984, 1986, 1987, and 1990, respectively, from Syracuse University, Syracuse, New York.

His research interests include computer networks, wireless communications and mobile computing, and optical networking. He currently serves on the editorial boards of six technical Journals and the Founder and EIC of "*Wireless Communications and Mobile Computing*" Journal published by John Wiley (http://www.interscience.wiley.com/jpages/1530-8669/). He is the author of eight books and more than 300 publications in refereed journals and conferences. He guest edited a number of special issues in IEEE Journals and Magazines. He also served as member, Chair, and General Chair of a number of conferences. Dr. Guizani served as the Chair of IEEE Communications Society Wireless Technical Committee (WTC) and Chair of Transmission, Access and Optical Systems (TAOS) Technical Committee. He was an IEEE Computer Society Distinguished Lecturer from 2003 to 2005. He is an IEEE Fellow and a Senior member of ACM.