

## An Efficient Data Transmission with Digital Signature in CWSNs



**Jeevitha.A**, M.E.student, Nandha Engineering College, Erode  
jeevithabe101291@gmail.com

**Satheeshkumar.S**, Assistant Professor/CSE, Nandha Engineering College, Erode,  
Sathishkumar1986@gmail.com

**Abstract** : 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. Secure and efficient data transmission (SET) is, thus, especially necessary and is demanded in many such practical WSNs. Cluster-based data transmission in WSNs has been investigated by researchers to achieve the network scalability and management, which maximizes node lifetime and reduce bandwidth consumption by using local collaboration among sensor nodes. In a cluster-based WSN (CWSN), every cluster has a leader sensor node, regarded as clusterhead (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).

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 results show that the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

**Keywords:** CWSNs, Secure efficient data transmission

### 1. INTRODUCTION

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 (SET) is, thus, especially necessary and is demanded in many such practical WSNs.

Cluster-based data transmission in WSNs has been investigated by researchers 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 clusterhead (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).

We propose two Secure and Efficient data Transmission 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 cryptosystems.

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 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 3 describes the network architecture, security vulnerabilities, and objectives. Section 4 introduces the IBS and IBOOS schemes for CWSNs. Sections 5 and 6 present the details of the proposed SET-IBS and SET-IBOOS, respectively, and Section 7 presents the protocol features and characteristics. Section 8 analyzes and evaluates the proposed SET-IBS and SET-IBOOS. The last section concludes this work.

## **2. RELATED WORK**

The low-energy adaptive clustering hierarchy (LEACH) protocol presented by Heinzelman et al. [4] is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. 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. 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 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, for example, 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 predistribution set into WSNs, and some papers appeared in recent years [16], [17], [18]. The IBOOS scheme has been proposed 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]. The offline signature in these schemes, however, is pre-computed by a third party and lacks reusability, thus they are not suitable for CWSNs. 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 an efficient secure data communication for CWSNs.

### 3. SYSTEM DESCRIPTION AND PROTOCOL OBJECTIVES

Here presents the network architecture, security vulnerabilities, and protocol objectives.

#### 1) Network Architecture

Consider a CWSN consisting of a fixed 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 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 time-division multiple access (TDMA) 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) 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]. 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, for example, pretend as a leaf node sending bogus information toward the CHs. Nevertheless, LEACH-like protocols are more robust against insider attacks than other types of protocols in WSNs. 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 (i.e., CH nodes).

The goal of the proposed secure data transmission for CWSNs is to guarantee the secure and efficient data transmissions 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], [9], [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 IDbased cryptosystem 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.

## 4. IBS AND IBOOS FOR CWSNS

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 first. To further reduce the computational overhead in the signing and verification process of the IBS scheme, we adapt the conventional IBOOS scheme for CWSNs.

### 1. Pairing for IBS

For self-contained, we briefly review the characteristics of pairing. Boneh and Franklin 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  $E/F_p$  indicate an elliptic curve  $y^2 = x^3 + ax + b$  ( $4a^3 + 27b^2 \neq 0$ ) over a finite field  $F_p$ . We denote by  $G_1$  a  $q$ -order subgroup of the additive group of points in  $E/F_p$ , and  $G_2$  a  $q$ -order subgroup of the multiplicative group in the finite field  $F_p$ . The pairing is a mapping  $e : G_1 \times G_2 \rightarrow G_2$ , which is a bilinear map with the following properties:

1. Bilinear.  $P, Q, R, S \in G_1, e(P + Q, R + S) = e(P, R) e(P, S) e(Q, R) e(Q, S)$ .
2. Nondegeneracy. If  $P$  is a generator of  $G_1$ , then  $e(P; P)$  is a generator of  $G_2$ .
3. Computability. There is an efficient algorithm to compute  $e(P, Q)$  in  $G_2, P, Q \in G_1$ .

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. A bilinear map  $e$  is secure if, given  $g; G; H \in G_1$ , it is hard to find  $h \in G_1$  such that  $e(h, H) = e(g, G)$ . Weil pairing and Tate pairing are the examples of such bilinear mapping, which present comprehensive descriptions of how pairing parameters can be selected for security.

### 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  $sekID$  associated with the ID using  $msk$ .

**Signature signing.** Given a message  $M$ , time stamp  $t$  and a signing key  $sk$ , 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.

### 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  $sekID$ ,  $SIG_{offline}$  and message  $M$ , a sending node (leaf node) generates an online signature  $SIG_{online}$ .

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

## 5.THE PROPOSED SET-IBS PROTOCOL

We propose two novel 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

### 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 predistribution is an efficient method to improve communication security, which has been adapted in WSNs in the literature [8], [9], [10], [15],

[16], [17], [18]. In this paper, we adopt IDkt as user's public key under an IBS scheme, 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 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 predistribution 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  $(p, q, E=F_p, G_1, G_2, e)$ , as described in Section 3. Select a generator  $P$  of  $G_1$  stochastically.
- Choose two cryptographic hash functions:  $H$ , for the point mapping hash function which maps strings to elements in  $G_1$ , and  $h$ , for mapping arbitrary inputs to fixed-length outputs.

### 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. We denote the ciphertext of the encrypted message as  $C$ . We adapt the algorithms of the IBS scheme from 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.

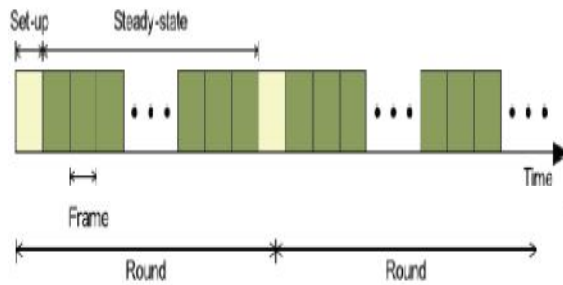
$$c_j = h(C_j || t_j || \theta_j), \quad (1)$$

... Let

$$\sigma_j = c_j s e k_j + \alpha_j P, \quad (2)$$

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



**Figure.1 Operation in the proposed method**

The operation of SET-IBS is divided by rounds as shown in Fig. 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 control [4]. Sensor nodes transmit the sensed data to the CHs in each frame of the steady-state phase. 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.

### 6. THE PROPOSED SET IBOOS PROTOCOL

We present the 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.

#### 1. Protocol Initialization

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; The BS does the following operations of key predistribution in the network:

Generate an encryption key  $k$  for the homomorphic encryption scheme to encrypt data messages, where  $k \in \mathbb{Z}_m - 1$ ,  $m$  is a large integer.

Let  $G$  be a multiplicative finite cyclic group with order  $q$ . The PKG selects a random generator  $g$  of group  $G$  generation, and chooses  $r \in \mathbb{Z}_q$  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

### 7. PROTOCOL FEATURES

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:

1. 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.

2. 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.

3. 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.

### 1. Protocol Characteristic

**Key management.** the key cryptographies used in the protocol to achieve secure data transmission, which consist of symmetric and asymmetric keybased 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, “comparatively 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.

## 2. Secure Data Transmission with Hierarchical Clustering

In large-scale CWSNs, multihop data transmission is used for transmission between the CHs to the BS, The version of the proposed SET-IBS and SET-IBOOS protocols for CWSNs can be extended using multihop 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 multihop planar model. A CH node transmits data to the BS by forwarding its data to its neighbour nodes, in turn the data are sent to the BS. We have proposed an energy-efficient routing algorithm for hierarchically clustered WSNs, 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, for example.

## 8. 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. 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 first node dies (FND), 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.

We apply confidence intervals to the simulation results, and a certain percentage (confidence level) is set to 90 percent. Shows the comparison of system lifetime using SET-IBS and SET-IBOOS versus LEACH protocol and SecLEACH 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.

## 9. CONCLUSION

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 results show that the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

## REFERENCES

- [1] T. Hara, V.I. Zadorozhny, and E. Buchmann, *Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence*, vol. 278. Springer-Verlag, 2010.
- [2] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," *IEEE Comm. Surveys & Tutorials*, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.
- [3] A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks," *Computer Comm.*, vol. 30, nos. 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 Comm.*, vol. 1, no. 4, pp. 660- 670, Oct. 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 & Distributed Systems*, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.
- [6] S. Yi et al., "PEACH: Power-Efficient and Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks," *Computer Comm.*, vol. 30, nos. 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'l J. Computer Applications*, vol. 47, no. 11, pp. 23-28, 2012.
- [8] L.B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks," *Signal Processing*, 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," *Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA)*, pp. 145-152, 2007.
- [10] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," *Proc. Fourth Int'l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM)*, pp. 1-5, 2008.
- [11] S. Sharma and S.K. Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks," *Proc. Int'l Conf. Comm., Computing & Security (ICCCS)*, pp. 146-151, 2011.
- [12] Gaubatz et al., "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks," *Proc. IEEE Third Int'l Conf. Pervasive Computing and Comm. Workshops (PerCom)*, pp. 146-150, 2005.
- [13] Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Trans. Information Theory*, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.
- [14] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," *Proc. Advances in Cryptology (CRYPTO)*, pp. 47-53, 1985.
- [15] D.W. Carman, "New Directions in Sensor Network Key Management," *Int'l J. Distributed Sensor Networks*, 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," *Proc. IEEE Int'l Conf. Computer and Information Technology (CIT)*, pp. 882-889, 2010.
- [17] H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID-Based Digital Signature," *Proc. IEEE GLOBECOM*, pp. 1-5, 2010.
- [18] J. Sun et al., "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," *IEEE Trans. Parallel & Distributed Systems*, vol. 21, no. 9, pp. 1227-1239, Sept. 2010.
- [19] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures," *Proc. Advances in Cryptology (CRYPTO)*, pp. 263-275, 1990.
- [20] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security," *Proc. 11th Australasian Conf. Information Security and Privacy*, pp. 99-110, 2006.