International Journal of Advanced Technology and Innovative Research

ISSN 2348–2370
Vol.07,Issue.05,
June-2015,
Pages:0648-0656

www.ijatir.org

Secure and Efficient Data Transmission for Cluster Based Wireless Sensor Networks

P. PRASANNA KUMARI[1], P. BHASKAR REDDY[2]

[1]PG Scholar, Dept of CSE, RVPECW, Kadapa, AP, India, Email: pkumari77@gmail.com.
[2]Assoc Prof, Dept of CSE, RVPECW, Kadapa, AP, India, Email: Bhaskar0308@gmail.com.

Abstract: In the past few years secure transmission of data along with efficiency is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and convenient way to enhance performance of the WSNs system. 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 In this project work, we study a secure transmission of data for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and sporadically,periodically. We make use of two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by means of the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, correspondingly. In this paper, after rigorous practical and theoretical analysis, we have designed efficient protocols to provide defense against innumerable security attacks in the clustered wireless sensor deployment environments. We have tried to address challenges like communication and computation overhead along with security to increase the performance of the deployed sensors. 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.

- Most existing time synchronization schemes are vulnerable to several attacks.
- Their low costs impede use of expensive tamper-resistant hardware.

Existing solutions are provided for distributed WSNs, but not for CWSNs.It reduces the possibility of a node joining with a CH.Problem occurs when a node does not share a pairwise key with others in its preloaded key ring. In the proposed protocols pairing parameters are distributed and preloaded in all sensor nodes by the BS initially. It overcomes the key escrow problem of the ID-based cryptosystem and is efficient in communication and saves energy. And Solve the orphan node problem in the secure data transmission with asymmetric key management and is more feasible.

Keywords: Cluster-Based WSNS, ID-Based Digital Signature, ID-Based Online/Offline Digital Signature, Secure Data Transmission Protocol.

I. INTRODUCTION

A Wireless sensor network (WSN) is a system of network comprised of spatially distributed devices using wireless sensor nodes to examine environmental or physical conditions, such as temperature, sound and movement. The individual nodes are competent of sensing their environments, processing the information statistics in the vicinity, and sending data to one or more compilation points in a WSN. Efficient transmission of data is one of the most significant issues for WSNs. Usually many WSNs are installed in unobserved, harsh and often adversarial physical environments for specific applications, such as armed forces domains and sensing tasks with unreliable surroundings. Efficient and secure transmission of data is thus very essential and is required in many such realistic WSNs. Cluster-based transmissions of data in WSNs, has been examined by researchers in order to accomplish the network scalability and supervision, which maximizes node life span and reduces bandwidth utilization by using local cooperation between sensor nodes. In a cluster-based WSN (CWSN), each cluster has a leader sensor node, known as cluster-head (CH). A CH collects the data gathered by the leaf nodes (non- CH sensor nodes) in its cluster, and sends the pooled data to the base station (BS).The probability of the asymmetric key management has been revealed in WSNs in recent times, which compensates the deficiency from relating the symmetric key management for security.

Digital signature is one of the most significant security services presented by cryptography in asymmetric key management systems, where the binding between the public key and the recognition of the signer is acquired via a digital certificate. The Identity-Based digital Signature (IBS) scheme, based on the complexity of factoring integers from Identity- Based Cryptography (IBC), is to develop an entity's public key from its character information, e.g., from its identification number or its name. This states that security must encompass every phase of the design of a wireless sensor network application that will require a high intensity of security. Probable applications comprise monitoring isolated or hostile locations, objective tracking in combat zone, catastrophe liberation networks, premature fire recognition, and environmental supervision. A primary topic that must be addressed when using cluster-based

security protocols based on symmetric session keys is the means used for ascertaining the session keys in the primary place. A vital design concern for security protocols based on symmetric keys is the degree of session key among the nodes in the system. On the other hand, it has the clear security drawback that the negotiation of a single node will disclose the global key.

A wireless sensor network (WSN) generally consists of a base station (or "gateway") that can communicate with a number of wireless sensors via a radio link. Data is collected at the wireless sensor node, compressed, and transmitted to the gateway directly or, if required, uses other wireless sensor nodes to forward data to the gateway. The transmitted data is then presented to the system by the gateway connection. The purpose of this chapter is to provide a brief technical introduction to wireless sensor networks and present a few applications in which wireless sensor networks are enabling. A WSN usually consists of tens to thousands of such nodes that communicate through wireless channels for information sharing and cooperative processing. WSNs can be deployed on a global scale for environmental monitoring and habitat study, over a battle field for military surveillance and reconnaissance, in emergent environments for search and rescue, in factories for condition based maintenance, in buildings for infrastructure health monitoring, in homes to realize smart homes, or even in bodies for patient monitoring. After the initial deployment (typically ad hoc), sensor nodes are responsible for self-organizing an appropriate network infrastructure, often with multi-hop connection between sensor nodes. The onboard sensors then start collecting acoustic, seismic, infrared or magnetic Information about the environment, using either continuous or event driven working modes.

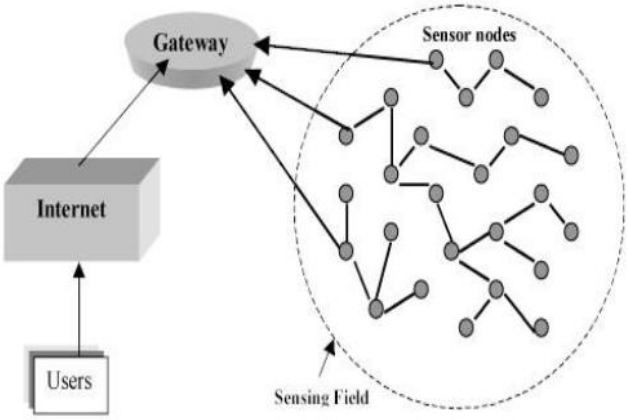

Fig.1. Architecture of WSN.

Recently, we have designed a secure and efficient data transmission protocol called SET-CTA for non-clustered environments which addresses all the challenges of non-clustered wireless sensor network deployment environment. In previously proposed SET-CTA scheme, we have used symmetric encryption scheme, ID based authentication scheme using Elliptic Curve Cryptography algorithm (ECC) and also managed concurrency and session establishment between end-end sensor nodes. In this paper, we extend our previous work and focus on providing efficient secure data communication for CWSNs and we have also removed orphan node problem by using asymmetric key management scheme. Moreover, in this proposed scheme, we have made an arrangement to switch the sensor nodes in in-active mode when they are not processing any data or performing any computations using timestamp based scheme.

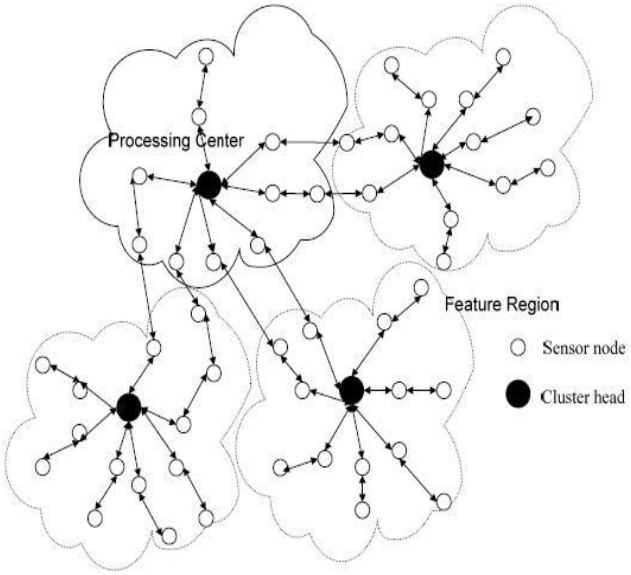

Fig1. System Architecture.

The remainder of this paper is organized as follows: SectionII describes the Related Work. SectionIII introduces the Cluster Network Model. SectionIV analyzes and evaluates the proposed SET-IBS and SET-IBOOS. In finally sectionIV gives the conclusions of this paper.

WSN security challenges:

- Conflicting between minimization of resource consumption and maximization of security level.
- Advanced anti-jamming techniques are impossible due to its complex design and high energy consumption. .
- Ad-hoc topology facilitates attackers of different types and from different directions.
- Most current standard security protocols do not scale to a large number of participants.
- Encryption requires extra processing, memory and battery power.
- Secure asymmetric key needs more computations.
- Although sensors location information are important most of current proposal are suitable for static WSNs.
- Most existing time synchronization schemes are vulnerable to several attacks.
- Their low costs impedes use of expensive tamper-resistant hardware.
- Little research has been done in code attestation.

II. RELATED WORK

In this proposed work a networking together hundreds or thousands of cheap micro-sensor nodes allows users to accurately monitor a remote environment by intelligently combining the data from the individual nodes. These networks require robust wireless communication protocols that are energy efficient and provide low latency. They develop and analyze low-energy adaptive clustering hierarchy (LEACH), a protocol architecture for micro-sensor networks that combines the ideas of energy-efficient cluster-based routing and media access together with application-specific data aggregation to achieve good performance in terms of system lifetime, latency, and application-perceived quality. LEACH includes a new, distributed cluster formation technique that enables self-organization of large numbers of nodes, algorithms for adapting clusters and rotating cluster head positions to evenly distribute the energy load among all the nodes, and techniques to enable distributed signal processing to save communication resources. The results show that LEACH can improve system lifetime by an order of magnitude compared with general-purpose multi-hop approaches. It was shown to increase system throughput, decrease system delay, and save energy while performing data aggregation.

Whereas those with rotating cluster heads, such as LEACH have also advantages in terms of security, the dynamic nature of their communication makes most existing security solutions inadequate for them. In this paper, they investigate the problem of adding security to hierarchical (cluster-based) sensor networks where clusters are formed dynamically and periodically, such as LEACH. For this purpose, we show how random key pre-distribution, widely studied in the context of flat networks. Increased interest in the potential use of wireless sensor networks (WSNs) in applications such as disaster management, combat field reconnaissance, border protection and security surveillance Sensors in these applications are expected to be remotely deployed in large numbers and to operate autonomously in unattended environments. To support scalability, nodes are often grouped into disjoint and mostly non-overlapping clusters. In this they presented a taxonomy and general classification of published clustering schemes. They survey different clustering algorithms for WSNs; highlighting their objectives, features, complexity, etc. We also compare of these clustering algorithms based on metrics such as convergence rate, cluster stability, cluster overlapping, location awareness and support for node mobility.

Security in a WSN is extremely important. Moreover, it should be run reliably without interruption.

1. Security requirements:
   - Confidentiality.
   - Authentication.
   - Non-repudiation .
   - Integrity.
   - Freshness
   - Forward and Backward secrecy

2. Survivability requirements:
   - Reliability
   - Availability.
   - Energy efficiency.

A. 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.

B. IBS scheme

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

C. IBOOS Scheme

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

D. Key Management

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.

III. CLUSTER NETWORK MODEL

Fig.2 shows the simple cluster Network Architecture, In Cluster Network; consist of large number of Sensor Nodes (SN) are grouped into different clusters. Each Cluster is composed of one Cluster Head (CH) sensor node which is elected autonomously and cluster member nodes or leaf (non CH). Leaf (non CH), join a cluster depending on the receiving signal strength. The Cluster Head (CH) gets the

sensed data from the leaf (non CH), aggregates the sensed information and then sends it to the base station.

Clustered Architecture:

- Organizes the sensor nodes into clusters
- Each cluster is governed by a cluster-head
- Only heads send messages to a BS
- Suitable for data fusion
- Self-organizing

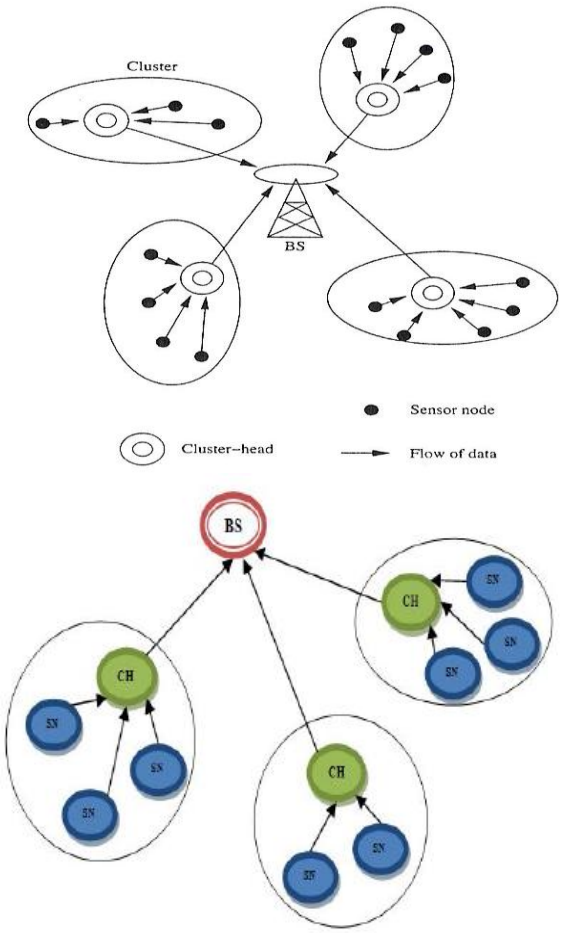

Fig.2. Simple Cluster Network Architecture

In Cluster wireless sensor networks have the following characteristics:

1. **It includes two kinds of nodes:** Sensor nodes with limited energy can sense their own residual energy and have the same architecture. Base Station (BS) without energy restriction is far away from the area of sensor nodes.
2. All sensor nodes use the direct transmission or multi-hop transmission to communicate with the BS.
3. Sensor nodes sense environment at a fixed rate and always have data to send to the BS.
4. Cluster head perform data aggregation and Base Station (BS) receives compressed data.
5. The lifespan of WSN is the total amount of time before the first sensor node runs out of power.
6. Some very big clusters and very small clusters may exist in the network at the same time.

A. Advantages:

1. Data aggregation process we can enhance the secure, robustness and accuracy of information which is obtained by entire network, certain redundancy exists in the data collected from sensor nodes thus data fusion processing is needed to reduce the redundant information.
2. Another advantage is those reduces the traffic load and conserve energy of the sensor.

B. Disadvantages:

1. The Cluster Head (CH) send fuse these data to the base station .This Cluster Head (CH) may be attacked by malicious attacker. If a cluster head is compromised, then the base station (sink) cannot be ensure the correctness of the aggregate data that has been send to it.
2. In existing systems are several copies of the aggregate result may be sent to the base station (sink) by uncompromised nodes .It increase the power consumed at these nodes.
3. Sensor nodes are having normal battery life and Cluster Head (CH) having high battery life time as compared with sensor nodes.

C. Leach Protocol Operation

Clustered WSNs were first proposed for various reasons including scalability and energy efficiency. The LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol presented by 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. Adding security to LEACH-like protocols is challenging, because they dynamically, randomly and periodically rearrange the network's clusters and data links. Therefore, providing steady long-lasting node-to-node trust relationships and common key distributions are inadequate for LEACH-like protocols. In this paper, we focus on providing efficient security to pair wise node-to-CH communications in LEACH-like protocol. Our main contribution is to have provided an efficient solution for securing pair wise communications in LEACH.

We introduce the original LEACH protocol, and discuss its vulnerabilities. LEACH (Low Energy Adaptive Clustering Hierarchy) was proposed to balance energy among nodes. It assumes that every node can directly reach a BS by transmitting with high enough power. However, to save energy, sensor nodes (SN) send their messages to their CHs, which then aggregate the messages, and send the aggregate to the BS. To prevent energy drainage of a restricted set of CHs, LEACH randomly rotates CHs among all nodes in the network, from time to time, thus distributing aggregation- and routing-related energy consumption among all nodes in the network. LEACH thus works in rounds. In each round, it uses a distributed algorithm to elect CHs automatically and

dynamically cluster the remaining nodes around the CHs. The resulting clustering structure is used by all sensor-BS communications for the remaining of the round.

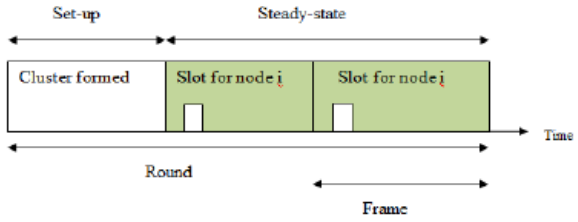

Fig.3. LEACH Protocol Operation

Merits:

- Accounting for adaptive clusters and rotating cluster heads
- Opportunity to implement any aggregation function at the cluster heads

Demerits:

- Highly dynamic environments
- Continuous updates and Mobility

LEACH Protocol operates in rounds during communication Rounds and have predetermined duration as shown in Fig 3, LEACH Protocol operation consists of two phases:

1. Set-up phase
2. Steady-state phase.

1. Set-up phase:
The setup consists of three steps.

Step 1: Sensor nodes decide probabilistically whether or not to become a CH for the current round (based on its remaining energy and a globally known desired percentage of CHs). The Cluster head (CH) broadcast the message to the set of all sensor nodes in the network.

During the setup phase, a predetermined fraction of nodes p, elect themselves as CHs as follows.

- A sensor node chooses a random number r, between 0 and 1. If this random number is less than a Threshold value, T (n), the node becomes a CH for the current round.
- The threshold value is calculated based on an equation that incorporates the desired percentage to become a CH, the current round, and the set of nodes that have not been selected as a CH in the last (1/p) rounds denoted as G.
- It is given by T (n) = p/ (1-p (mod (1/p)))

if n € G, where G is the set of nodes that are involved in the CH election.

Step2 (cluster joining step): All elected CHs broadcast an advertisement message to the rest of the sensor nodes in the Network that they are the new CHs. All the non-CH nodes, after receiving this advertisement, decide on the cluster to which they want to belong. This decision is based on the signal strength of the advertisement and communicates their intention to join by sending a join req (join request) message. The non-CH nodes inform the appropriate CHs that they will be a member of the cluster. After receiving all the messages from the sensor nodes that would like to be included in the cluster and based on the number of nodes in the cluster, the CH node creates a TDMA (Time Division Multiple Access) schedule and assigns each sensor node a time slot when it can transmit. This schedule is broadcast to all the nodes in the cluster. During the steady-state phase, the sensor nodes can begin sensing and transmitting data to the CHs. The CH node, after receiving all the data, aggregates it before sending it to the Base station (BS). After a certain time, which is determined a priori, the network goes back into the set-up phase again and enters another round of selecting new CHs.

Step3:(confirmation step): It starts with the CHs broadcasting a confirmation message that includes a time slot schedule to be used by their cluster members (Sensor nodes) for communication during the steady-state phase.

2. Steady-State Phase

Once the clusters are set up, the network moves on to the steady-state phase, where actual communication between sensor nodes and the Base Station (BS) takes place

Step 4: Each Sensor node (SN) knows when it is its turn to transmit the data to the cluster head (CH) according to the time slot schedule.

Step 5: The CHs collect messages from all their Sensor nodes (SN) or cluster members, aggregate these data, and send the result to the BS. The steady-state phase consists on multiple reporting cycles, and lasts much longer compared to the set up phase.

Table 1. LEACH Protocol Operation ut

Set-up Phase
1. $CH \Rightarrow G_i$: id_{CH}, adv
2. $SN \rightarrow CH$: $id_{SN}, id_{CH}, join\_req$
3. $CH \Rightarrow G_i$: $id_{CH}(... <id_{SN}, t_{SN}>, ...), sched)$
Steady-State Phase
4. $SN_i \rightarrow CH$: id_{SN}, id_{CH}, d_{SN}
5. $CH \rightarrow BS$: $id_{CH}, id_{BS}, F(.. d_{SN} ..)$

IV. IBS SCHEME FOR CWSNs

IBS Scheme implemented for CWSNs consists of the following operations.

1. **Setup:** The BS generates a master key and public parameters for the private key generator and gives them to all sensor nodes.

2. **Extraction:** Given an Id string ,a sensor node generates a private key associated with the id using master key.

3. **Signature signing:** Given a message ,time stamp and a signing key the sending node generates a signature.

4. **Verification:** Given the id,msg and signature,the receiving node outputs accept if signature is valid and outputs reject otherwise.

A. IBOOS Scheme for CWSNs

IBOOS Scheme implemented for CWSNs consists of the following operations.

1. Setup: The BS generates a master key and public parameters for the private key generator and gives them to all sensor nodes.
2. Extraction: Given an Id string ,a sensor node generates a private key associated with the id using master key.
3. Offline signing: Given a public parameters, time stamp the CH sensor node generates an offline signature and transmits it to the leaf nodes in its cluster.
4. Online signing: From the private key,offline signature and message ,a sending node generates an online signature.
5. Verification: Given the id,msg and signature,the receiving node outputs accept if signature is valid and outputs reject otherwise.

B. Operations in SET-IBS

1. Setup phase:

- The BS broadcasts its information to all nodes.
- The elected CHs broadcasts their information.
- A leaf node joins a cluster of the CH i.
- A CH I broadcast the schedule message to its members.

2. Steady state phase:

- A leaf node j transmits the sensed data to its CH i.
- A CH i transmits the aggregated data to the BS.

C. Operations in SET-IBOOS

1. Setup phase:

- The BS broadcasts its information to all nodes.
- The elected CHs broadcasts their information.
- A leaf node joins a cluster of the CH i.
- A CH i broadcast the allocation message

2. Steady state phase:

- A leaf node j transmits the sensed data to its CH i.
- A CH I transmits the aggregated data to the BS.

D. Characteristics of the Prior Protocols:

1. Key management is Symmetric.
2. Neighborhood authentication is limited.
3. Storage cost is high.
4. Networks scalability is low.
5. Communication overhead is probabilistic.
6. Computational overhead is low.
7. Attack resilience is passive and active attacks on wireless channels.

E. Characteristics of the Proposed Protocols:

1. Key management is asymmetric.
2. Neighborhood authentication is not limited.
3. Storage cost is low.
4. Networks scalability is high.
5. Communication overhead is deterministic.
6. Computational overhead is high.
7. Attack resilience is passive and active attacks on wireless channels

IV. PROTOCOL EVALUATION

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 to simulate SET-IBS and SET-IBOOS, and we focus on the energy consumption spent on message propagation and computation.

A. Security Analysis

To evaluate the security of the proposed protocols, we have to investigate the attack models in WSNs that 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.

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 [3].
- **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, for example, 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.

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 are encrypted by the homomorphic encryption scheme from, 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 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 SETIBOOS works 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 fulfill 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, 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 predefined 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. 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 nodes 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.

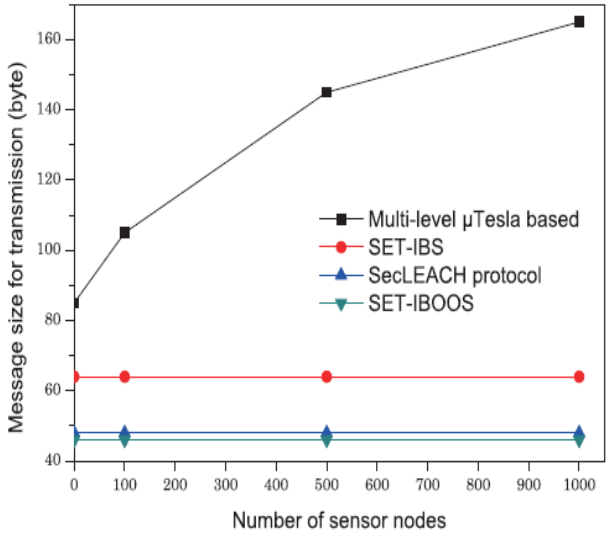

Fig.4. Message size for transmission compared to the number of nodes.

Fig.4 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 multilevel μ Tesla-based protocol. At the same time, it generates larger message size as compared to SecLEACH. However, the orphan node problem is fully solved in SETIBS. 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 section.

C. 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 SETIBOOS. 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 [5] and SecLEACH protocol [9].. 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 [2]. 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 100 m ×100 m area, with a fixed BS located near part of the area, as shown in the figure in the Appendix. 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, for example, Crossbow Stargate.

Table2. 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 $E_{receive}$	$28.6\mu J/byte$

Table 2 lists up the parameter settings for the energy consumption in the network simulations. In the simulations, we use the same radio energy model in [5], and the other parameters are from [9]. We assume that the BS has unlimited energy. For clustering, we properly set the desired percentage of CH nodes ρ =¼ 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 Ps = 0.87, which are also referred to as the expected orphan rate of the orphan node problem.

Fig.5 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 percent. Fig.7 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.

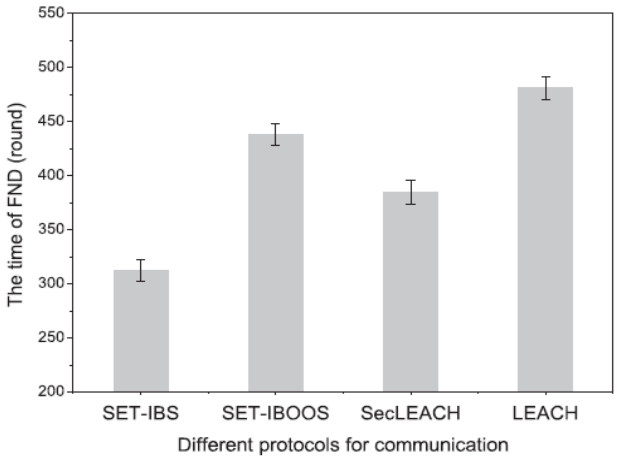

Fig.5. Comparison of FND time in different protocols

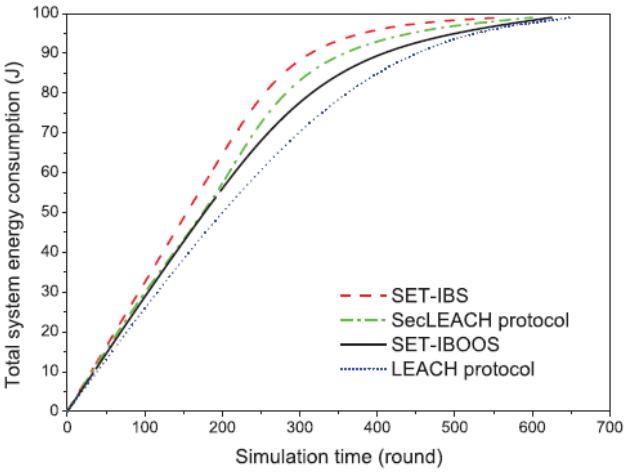

Fig.6. Comparison of energy consumption in different protocols.

Fig.6 illustrates the energy of all sensor nodes disseminated in the network, which also indicates the balance of energy consumption in the network. Fig. 7 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.

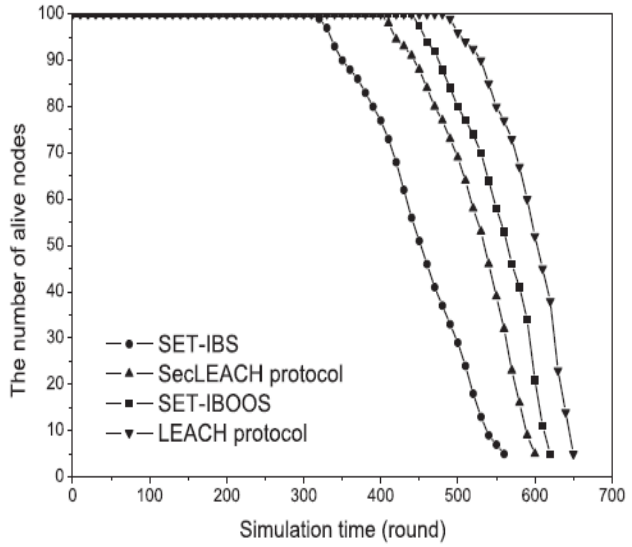

Fig.7. Comparison of the number of alive nodes in different protocols

V. CONCLUSION

In this paper, the data transmission issues and the security issues in CWSNs. 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. In future, we are planning to propose the similar kind of solutions for the decentralized wireless sensor environments.

VI. REFERENCES

[1] Huang Lu, Student Member, IEEE, Jie Li, Senior Member, IEEE, and Mohsen Guizani, Fellow, IEEE, "Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 3, March 2014.

[2] 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.

[3] 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.

[4] 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.

[5] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Micro-sensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670, Oct. 2002.

[6] 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.

[7] 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.

[8] 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.

[9] L.B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks," Signal Processing, vol. 87, pp. 2882-2895, 2007.

[10] 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.

[11] 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 (Wi-COM), pp. 1-5, 2008.

[12] 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.