ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

Preventing Data Transmission from Vulnerable Attacks in CWSNs

Anuradha Patnala[1], P.Hema Venkataramana[2]

[1] PG Scholar, Dept of CSE, Kakinada Institute of Engineering and Technology for Women (KIETW), India,

[2] M.Tech, Assistant Professor, Dept of CSE, Kakinada Institute of Engineering and Technology for Women (KIETW), India

ABSTRACT: The use of wireless sensor networks (WSNs) has grown enormously in the last decade, pointing out the crucial need for scalable and energy-efficient routing and data gathering and aggregation protocols in corresponding large-scale environments. Clustering is an effective and practical way to enhance the system performance of WSNs. In Cluster-based Wireless Sensor Networks identifying the various types of attacks is main problem. 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 and we proposed The Concentric Clustering Scheme (CCS) has been proposed to reduce the energy consumption loopholes in PEGASIS (Power-Efficient. Gathering in Sensor Information Systems).The main idea of CCS is to consider the location of the BS to enhance its performance and to prolong the lifetime of the network. Along with mainly we proposed 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.

KEYWORDS: Cluster, WSNs, Concentric, SET-IBS, SET- IBOOS, Secure Data Transmission Protocol.

I. INTRODUCTION

Wireless sensor network 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 wireless sensor network. Reliable data transmission is one of the most important issues for wireless sensor networks. Meanwhile, many wireless sensor networks are deployed in harsh, neglected and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trust less surroundings. Reliable data transmission is thus especially necessary and is demanded in many such practical wireless sensor networks.

A. Research Motivation

The typical clustering routings protocols in WSNs include Low-energy Adaptive Clustering Hierarchy (LEACH) [14], Hybrid Energy-Efficient Distributed clustering (HEED) [15], Distributed Weight-based Energy-efficient Hierarchical Clustering protocol (DWEHC) [16], Position-based Aggregator Node Election protocol (PANEL) [17,18], Two-Level Hierarchy LEACH (TL-LEACH) [19], Unequal Clustering Size (UCS) model [20], Energy Efficient Clustering Scheme (EECS) [21,22], Energy-Efficient Uneven Clustering (EEUC) algorithm [23], Algorithm for Cluster Establishment (ACE) [24], Base-Station Controlled Dynamic Clustering Protocol (BCDCP) [25], Power-Efficient Gathering in Sensor Information Systems (PEGASIS) [26], Threshold sensitive Energy Efficient sensor Network protocol (TEEN)[27], The Adaptive Threshold sensitive Energy Efficient sensor Network protocol

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

(APTEEN) [28], Two-Tier Data Dissemination (TTDD) [29], Concentric Clustering Scheme (CCS) [30], Hierarchical Geographic Multicast Routing (HGMR) [31], and etc. Clustering routing is becoming an active branch of routing technology in WSNs on account of a variety of advantages, such as more scalability, data aggregation/ fusion, less load, less energy consumption, more robustness, etc.

In the last few years, a relatively large number of clustering routing protocols have been developed for WSNs. This paper is an attempt to comprehensively review and critically discuss the most prominent clustering routing algorithms that have been developed for WSNs. The goals of this survey can be summarized as follows: (1) To make a large audience aware of the existence and of the usually good performance of a number of clustering routing protocols in WSNs; (2) To facilitate the reading as well as to provide a sound framework by a detailed taxonomy of clustering routing algorithms; (3) To highlight a few strengths and weaknesses of the proposed algorithms with respect to the performance of the clustering routing methods in WSNs; (4) To help application designers identify alternative solutions and select appropriate strategies by comparison of different clustering routing approaches. Recently, a few surveys of clustering routing methods for WSNs have been presented. These surveys mainly aim at outlining some characters of clustering and summarizing some popular clustering routing algorithms with comparison based on different attributes and performances. In this study, we present a comprehensive survey of different clustering routing protocols proposed in recent years. Our work differs from other surveys of WSN

II. RELATED WORK

These clustering approaches were compared based on a few metrics such as convergence rate, cluster stability, cluster overlapping, location-awareness and support for node mobility. [33] a comparison survey between different clustering protocols. The authors of the survey discussed some basic concepts related to the clustering process, such as cluster structure, cluster types, clustering advantages, and briefly analyzed LEACH-based protocols as well as proactive and reactive algorithms in WSNs. The main characteristics of these protocols were compared and the evidences where they can be used currently were outlined. [34] the clustering algorithms available for WSNs and classified them based on the cluster formation parameters and CH election criteria. The authors of the survey also studied the key design challenges and discussed the performance issues related clustering protocols based on the classification of identity-based clustering algorithms, neighbourhood information based clustering algorithms, probabilistic clustering algorithms and biologically inspired clustering algorithms. Different clustering schemes are discussed [35], with special emphasis on their CH selection strategies based on the classification of deterministic scheme, adaptive scheme and combined metric scheme. The costs of CH selection were compared with respect to cluster formation, distribution of CHs and creation of clusters. Besides, a need of more scalable, energy efficient and stable clustering scheme for data gathering in WSNs was put forward. [36] A total of three prominent advantages of clustering methods for WSNs, such as more scalability, less overheads, and easy maintenance, and then present a classification of WSN clustering schemes based on a total of eight clustering attributes.

The authors also analyzed altogether six popular WSN clustering algorithms, such as LEACH, PEGASIS, HEED, EEUC, and etc., and compared these WSN clustering algorithms, including various attributes. [37] considered clustering routing protocols to achieve energy efficiency in WSNs and presented a review on clustering algorithms from the perspective of data routing. A simple classification of clustering routing protocols is proposed in the review. Totally nine typical clustering protocols including two classes, pre-established clustering routing algorithms and on-demand clustering routing algorithms, are summarized in respectively. Besides, some future research directions are presented in the review. The operations of some clustering protocols were discussed in the survey presented in [38], and the advantages and limitations of each one of these algorithms were analyzed in brief. The authors of the survey selected only seven popular clustering algorithms for WSNs, such as LEACH, TL-LEACH, EECS, TEEN, APTEEN, and etc. Additionally, the survey compared these clustering protocols in terms of energy consumption and network lifetime. [31] have made a simple survey of clustering routing protocols, including only six typical clustering algorithms. The authors of the survey simply compared these clustering routing algorithms based on some performance parameters, including energy conservation, network lifetime, data aggregation, robustness, scalability, security, and etc. Another simple survey on clustering routing algorithms was given by Joshi [32]. Only eight popular clustering routing protocols are covered in this survey, such as LEACH, PEGASIS, TEEN, APTEEN, etc.

The authors of the survey briefly compared these clustering routing approached based on energy conservation and the network lifetime. An overview of Haneef and Deng [33] focuses on design challenges and comparative analysis of

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

WSN clustering routing algorithms for improving the network lifetime. The authors of the overview analyzed many challenging factors that influenced design of routing protocols in WSNs, and presented a simple classification of routing protocols. Besides, many efficient clustering based classical WSN routing protocols with comparative analysis were discussed in the overview. 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. 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. 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, e.g., [16] and [17]. The IBOOS scheme has been proposed in order to reduce the computation and storage costs of signature processing. A general method for constructing online/o*ff*line signature schemes was introduced by Even et al. [18].

III. SYSTEM DESCRIPTION AND PROTOCOL OBJECTIVES

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

A. 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.

B. 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, 21]. 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 [21]. 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 in 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. 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 su*ff*ers 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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

scheme. Furthermore, SET-IBOOS is proposed to reduce the computational overhead in SET-IBS with the IBOOS scheme.

IV. THE PROPOSED SET-IBS PROTOCOL

In this paper, we propose two novel Secure and Efficient data Transmission (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 com-munication, 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.

A. 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_i 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, 15–17]. In this paper, we adopt $ID||t_i$ as user's public key under an IBS scheme [22], 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 [29] to encrypt the plaintext of sensed data, in which a specific operation performed on the plaintext is equivalent to the op-eration 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$_\epsilon$ key k for the homomorphic en-cryption scheme to encrypt data messages, where k $[m - 1]$, m is a large integer.
- Generate the pairing parameters $(p,q,E/F_p,G_1,G_2,e)$, as

  described in SectionIII, Select a generator P of G_1 stochastically.

- Choose two cryptographic hash functions: H, for point

  mapping hash function which maps strings to elements in G_1, and h, for mapping arbitrary inputs to fixed-length outputs$_\epsilon$.
- Pick a random integer τ Z_q as the master key msk, set $P_{pub} = \tau P$ as network public key.
- Preload each sensor node with the system parameters $param_1 = (k,m, p,q,E/F_p,G_1,G_2,e, H,h, P,\tau)$.

B. Key management for security

Assume that a sensor node j transmits a message M, and encrypts the data using the encryption key k from the additively homomorphic encryption scheme [29]. We denote the ciphertext of the encrypted message as C. In order to adapt the algorithms of IBS from[22] to WSNs practically, we simplify the mapping e with one generator P and providethe full algorithm in the signature verification. The IBS scheme in the proposed SET-IBS consists of following three operations, extraction, signing and verification. Extraction: It first obtains its private key as the time-stamp of the time interval in the current round from TDMA (time division multiple access) control. Signature signing: The sensor node picks a random number $\alpha \in Z$, computes $\theta = e(P, P)\alpha$. The sensor node further computes

$$c\,j = h(Cti\theta) \quad (1)$$

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

Let ,σj = c jsek j + αP , (2)

where σj, cj is the digital signature on the encrypted message C. The broadcast message is now concatenated in the form of (IDj, ti,C, σj, cj).

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

θ = e(σj,P) e(H(IDj,|| ti),-PPUB)Cj (3)

Using the time-stamp of current time interval ti and a random α for deriving θ , the sensor node does the bilinear transformation and mapping from θ to θ. We have the formula below if the received message is authentic

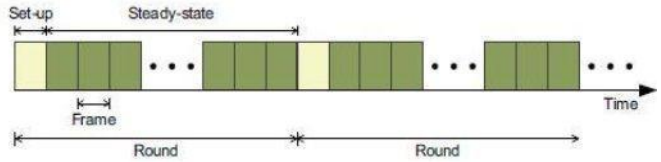
θ = e(σj,P) e(H(IDj,|| ti),-PPUB)Cj
=e(σj,P) e(H(IDj,|| ti),- τ P)
= e(cj sekj +α P, P) e(H(IDj,|| ti),- τ P)C
= e(cj sekj +α P, P) e(τ H(IDj,|| ti), P) (4)
=e(cj sekj , P)cj e(p,p)α e(τ H(IDj,|| ti), P)Cj = e(cj sekj , P)cj e(p,p)α e(cj sekj , P)-cj
= e(p,p)α = θ.

If h (Cti, θ) = h (Cti, θ) = cj , 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.

C. 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.



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 steadystate 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, SETIBS functions without data transmission with each other in the CH rotations. In the setup phase, the time- stamp Ts and node IDs are used for the signature generation. Whereas, in the steady-state phase, the time-stamp ti is used for the signature generation securing the inner cluster communications, and Ts 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 Ts 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:

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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

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., Ecur (n)Einit (n)) to increase the energy efficiency in the clustering, where, Ecur (n) is the current energy, and Einit (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., ρ=10%), r is the current round number, and Gn is the set of sensor nodes that have not been CHs in the last _1/ρ_ 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 (σi, ci).

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 IDi, its own ID IDj, time-stamp Ts, and the digital signature (σj, c j). In Step 4, a CH i broadcasts an allocation message to its cluster members for communication during the steady-state phase, including a time schedule sched by the TDMA control, yet to be concatenated with the signature. 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 in a packet (IDj, tj,C, σj, cj)to its CH, which is concatenated with a digital signature in a time slot tj, where the sender ID ID j with tj 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.

V. THE PROPOSED SET-IBOOS PROTOCOL

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 SETIBS, which has a protocol initialization prior to the network deployment and operates inrounds 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

A. 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 predistribution 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 [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 for group G generation, and chooses x Z, q at ϵrandom as the master secret key.

select r Z q for each node private key generation, and let H be a hash function.

Preload each sensor node with the public parameters given by param2=(k,m,G, q, g, x, r, H).

B. Key management for security

Assume that a sensor node j transmits a message M, and we denote the ciphertext of the encrypted message as C, which is encrypted by the same encryption scheme in SETIBS. Inspired from the concept of an IBOOS scheme [23], we construct an IBOOS scheme based on the DLP in the multiplicative group, and propose a novel secure data transmission protocol with IBOOS specifically for CWSNs (SET-IBOOS). The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. The IBOOS scheme in the proposed

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

SET-IBOOS consists of following four operations, extraction, offline signing, online signing and verification.

Extraction: Before the signature process, it first extracts private keys from the master secret key x and its identity ID, as sek=(R, si), where R = gr,

$$si = r + H(R, ID_i)x \bmod q. \quad (6)$$

Offline signing: It generates the offline signature (σi) with the time-stamp of its time slot ti for transmission, and store the knowledge for signing online signature when it sends the message.

C. Protocol operation

The proposed SET-IBOOS operates similarly to that of SETIBS. 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. For the IBOOS key management in SET-IBOOS, the offline signatures are generated by the CHs, which are used for the online signing at the leaf nodes. Table II 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 IBOOS is similar to that in INS. However, the difference in steps 2 and 3 is the change from the IBS to the online signature _σi, zi_ of the IBOOS scheme. In Step 4, a CH i first generates the offline signatures for the leaf nodes in its cluster, respectively. It then broadcasts an allocation message (alloc(IDj/tj/σ j)) to its cluster members for the secure communication during the steadystate phase, yet to concatenated with the online signature. The allocation message consists of a time schedule composed by the TDMA control, which allocates a time-stamp with an offline signature IDj/tj/ σ j for node j. 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 I, where the IBS is changed into the online signature of the IBOOS scheme.

VI. PROTOCOL FEATURES

The protocol characteristics and hierarchical clustering solutions are presented in this section.

A. Protocol Characteristics

In this part, we summarize the characteristics of the proposed SET-IBS and SET-IBOOS protocols. Table III 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.

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 ableto 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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

B.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 SETIBOOS 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 [30], 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., [31].

VII. 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. We focus on the energy consumption spent on message propagation and computation. We use the network simulator OMNeT++ 3.0 to simulate the proposed SET-IBS and SET-IBOOS, and the simulation source code can be found in [32].

A. 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.

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, 21].

- ∑ 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.

2. CCS

The Concentric Clustering Scheme (CCS) has been proposed in [30] by Jung et al. to reduce the energy consumption loopholes in PEGASIS (Power Efficient. Gathering in Sensor Information Systems), The main idea of CCS is to consider the location of the BS to enhance its performance and to prolong the lifetime of the network. In CCS, the network is divided into a variety of concentric circular tracks which represent different clusters and each circular track is assigned with a level. The track nearest to the BS is assigned with level-1 and the level number increases with the increase of the distance to the BS. Thus, each node in the network is assigned with its own level. Besides, chains are constructed within the track as that in PEGASIS. One of the nodes on the chain at each level area is

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

selected as a CH. A CH in level L is selected with node number obtained by calculating i mod ML, where ML represents the number of nodes that have the same level in i round. Data transmission in CCS is based on the process of PEGASIS protocol. After CH selection, each CH transmits the data of its own location to both the upper and lower level CH in one grade. In the process of the data transmission, all nodes in each level transmit the data to the nearest node from themselves along the chain.

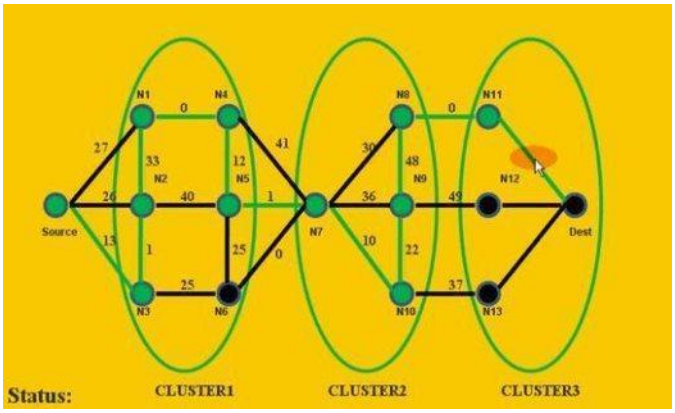


Fig1. Cluster Base Wireless Sensor Network.

The node receives the data and fuses its own data and transmits these data to the next node. Therefore, the CH receives at most two data messages. Subsequently, the CH in each level transmits the data to the lower CH. At last, level 1 CH transmits these data to the BS. The data transmission scheme in CCS is shown in Figure 1. Compared to PEGASIS, CCS embodies the advantaged as follows: (1) The distance over which the data can be transmitted to the BS from the CH is reduced in CCS. Hence, a considerable amount of energy is saved on account of the reduction of transmission distance in CCS [76]; (2) The network is divided into a series of concentric clusters, and the reverse data flow from the BS is also reduced. Thus, a considerable amount of energy is also conserved during data transmission. However, there are some disadvantages to be considered as follows: (1) Node distribution in each level is unbalanced, thus the levels with small number of nodes will deplete their energy first, in that the probability of election to be a CH is high; (2) Residual energy is not considered for CH election, which may lead to unbalanced energy consumption among all nodes; (3) Chain-based protocols, such as PEGASIS and CCS, enable nodes to communicate with their closest neighbour by using low radio power, but the long chain would cause large delay [7]; (4) The CH selection for next hop is based on the location rather than the residual energy of nodes, thus energy of CH may dissipates quickly on the path among CHs, and even energy hole will appear in the network.

B. 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.

VIII. CONCLUSION

In Cluster Wireless Sensor Networks transmitting data securely to the sender node to destination nodes is very big problem. In this paper we analyzed process of CWSN identified types of attacks and prevent data from attacks. 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. And CCS 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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

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.

REFERENCES

[1] T. Hara, V. I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Info. 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, 2006.
[3] A. A. Abbasi and M. Younis, ―A survey on clustering algorithms for wireless sensor networks,‖ Comput. Commun., vol. 30, no. 14-15, 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, 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, 2002.
[6] S. Yi, J. Heo, Y. Cho et al., ―PEACH: Power-efficient and adaptive clustering hierarchy protocol for WSNs,‖ Comput. Commun., vol. 30, no. 14-15, 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, 2012.
[8] L. B. Oliveira, A. Ferreira, M. A. Vilac¸a et al., ―SecLEACH-On the security of clustered sensor networks,‖ Signal Process., vol. 87, 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.
[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.
[11] S. Sharma and S. K. Jena, ―A survey on secure hierarchical routing protocols in wireless sensor networks,‖ in Proc. ICCCS, 2011.
[12] G. Gaubatz, J. P. Kaps, E. Ozturk et al., ―State of the Art in Ultra-Low Power Public Key Cryptography for WSNs,‖ in Proc. IEEE PerCom Workshops, 2005.
[13] D. Boneh and M. Franklin, ―Identity-Based Encryption from the Weil Pairing,‖ in Lect. Notes. Comput. Sc. - CRYPTO, 2001.
[14]. Heinzelman, W.R.; Chandrakasan, A.; Balakrishnan, H. Energy-Efficient Communication Protocol for Wireless Microsensor Networks. In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, HI, USA, 4–7 January 2000; pp. 10–19.
[15]. Younis, O.; Fahmy, S. HEED: A hybrid, energy-efficient, distributed clustering approach for ad-hoc sensor networks. IEEE Trans. Mobile Comput. **2004**, 3, 366–379.
[16]. Ding, P.; Holliday, J.; Celik, A. Distributed Energy Efficient Hierarchical Clustering for Wireless Sensor Networks. In Proceedings of the 8th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS), Marina Del Rey, CA, USA, 8–10 June 2005; pp. 322–339.
[17]. Buttyan, L.; Schaffer, P. PANEL: Position-Based Aggregator Node Election in Wireless Sensor Networks. In Proceedings of the 4th IEEE International Conference on Mobile Ad-hoc and Sensor Systems Conference (MASS), Pisa, Italy, 8–11 October 2007; pp. 1–9.
[18]. Buttyan, L.; Schaffer, P. PANEL: Position-based aggregator node election in wireless sensor networks. Int. J. Distrib. Sens. Netw. **2010**, 2010, 1–16.
[19]. Loscri, V.; Morabito, G.; Marano, S. A Two-Level Hierarchy for Low-Energy Adaptive Clustering Hierarchy. In Proceedings of the 2nd IEEE Semiannual Vehicular Technology Conference, Dallas, TX, USA, 25–28 September 2005; pp. 1809–1813.
[20]. Soro, S.; Heinzelman, W. Prolonging the Lifetime of Wireless Sensor Networks via Unequal Clustering. In Proceedings of the 5th IEEE International Workshop on Algorithms for Wireless, Mobile, Ad Hoc and Sensor Networks (WMAN), Denver, CO, USA, 4–8 April 2005; pp. 236–243.
[21]. Ye, M.; Li, C.; Chen, G.; Wu, J. EECS: An Energy Efficient Clustering Scheme in Wireless Sensor Networks. In Proceedings of the 24th IEEE International Performance, Computing, and Communications Conference (IPCCC), Phoenix, AZ, USA, 7–9 April 2005; pp. 535–540.
[22]. Ye, M.; Li, C.; Chen, G.; Wu, J. An energy efficient clustering scheme in wireless sensor networks. Ad Hoc Sens. Wirel. Netw. **2006**, 3, 99–119.
[23]. Li, C.F.; Ye, M.; Chen, G.H.; Wu, J. An Energy-Efficient Unequal Clustering Mechanism for Wireless Sensor Networks. In Proceedings of the 2nd IEEE International Conference on Mobile Ad-hoc and Sensor Systems Conference (MASS), Washington, DC, 7–10 November 2005; pp. 596–604.
[24]. Chan, H.; Perrig, A. ACE: An Emergent Algorithm for Highly Uniform Cluster Formation. In Proceedings of the 1st European Workshop on Sensor Networks (EWSN), Berlin, Germany, 19–21 January 2004; pp. 154–171.
[25]. Murugunathan, S.D.; Ma, D.C.F.; Bhasin, R.I.; Fapajuwo, A.O. A Centralized Energy-Efficient Routing Protocol for Wireless Sensor Networks. IEEE Radio Commun. **2005**, 43, S8–S13.
[26]. Lindsey, S.; Raghavendra, C.; Sivalingam, K.M. Data gathering algorithms in sensor networks using energy metrics. IEEE Trans. Parallel Distrib. Syst. **2002**, 13, 924– 935.
[27]. Manjeshwar, E.; Agrawal, D.P. TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks. In Proceedings of the 15th International Parallel and Distributed Processing Symposium (IPDPS), San Francisco, CA, USA, 23–27 April 2001; pp. 2009–2015.
[28]. Manjeshwar, A.; Agrawal, D. P. APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks. In Proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile computing, Lauderdale, FL, USA, 15–19 April 2002; pp. 195–202.
[29]. Luo, H.; Ye, F.; Cheng, J.; Lu, S.; Zhang, L. TTDD: Two-tier data dissemination in large-scale wireless sensor networks. Wirel. Netw. **2005**, doi:10.1007/s11276-004-4753-x.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

[30]. Jung, S.; Han, Y.; Chung, T. The Concentric Clustering Scheme for Efficient Energy Consumption in the PEGASIS. In Proceedings of the 9th International Conference on Advanced Communication Technology, Gangwon-Do, Korea, 12–14 February 2007; pp. 260–265.
[31]. Koutsonikola, D.; Das, S.; Charlie, H.Y.; Stojmenovic, I. Hierarchical geographic multicast routing for wireless sensor networks. Wirel. Netw. **2010**, 16, 449–466.
[32]. Abbasi, A.A.; Younis, M. A survey on clustering algorithms for wireless sensor networks. Comput. Commun. 2007, 30, 2826–2841.
[33]. Arboleda, L.M. C.; Nasser, N. Comparison of Clustering Algorithms and Protocols for Wireless Sensor Networks. In Proceedings of IEEE CCECE/CCGEI, Ottawa, ON, Canada, 7–10 May 2006; pp. 1787–1792.
[34]. Kumarawadu, P.; Dechene, D.J.; Luccini, M.; Sauer, A. Algorithms for Node Clustering in Wireless Sensor Networks: A Survey. In Proceedings of 4th International Conference on Information and Automation for Sustainability, Colombo, Sri Lanka, 12–14 December 2008; pp. 295–300.
[35]. Deosarkar, B.P.; Yada, N.S.; Yadav, R.P. Cluster Head Selection in Clustering Algorithms for Wireless Sensor Networks: A Survey. In Proceedings of the 2008 International Conference on Computing, Communication and Networking, Virgin Islands, USA, 3–7 August 2008; pp. 1–8.
[36]. Jiang, C.; Yuan, D.; Zhao, Y. Towards Clustering Algorithms in Wireless Sensor Networks— A Survey. In Proceedings of IEEE Wireless Communications and Networking Conference, Budapest, Hungary, 5–8 April 2009; pp. 1–6.
[37]. Maimour, M.; Zeghilet, H.; Lepage, F. Cluster-based Routing Protocols for Energy-Efficiency in Wireless Sensor Networks. Available online: http://cdn.intechweb.org/pdfs/12423.pdf (accessed on 14 December 2010).
[38]. Lotf, J.J.; Hosseinzadeh, M.; Alguliev, R.M. Hierarchical Routing in Wireless Sensor Networks: A Survey. In Proceedings of 2010 2nd International Conference on Computer Engineering and Technology, Chengdu, China, 16–18 April 2010; pp. 650–654.
[39]. Boyinbode, O.; Le, H.; Mbogho, A.; Takizawa, M; Poliah, R. A Survey on Clustering Algorithms for Wireless Sensor Networks. In Proceedings of 2010 13th International Conference on Network-Based Information Systems, Takayama, Japan, 14–16 September, 2010.

BIOGRAPHY

Anuradha. Patnala, is a PG Scholar, Dept of CSE, Kakinada Institute of Engineering and Technology for Women, India,

P.Hema Venkataramana is a well known Author and excellent teacher Received M.Tech (CSE) from JNTU is working as Assistant Professor , Department of Computer science engineering , Kakinada Institute of Engineering &Technology for women, korangi. She has 3 years of teaching experience. Her areas of Interest include, information security, cloud computing Data mining and other advances in computer Applications.