A SECURE DATA TRANSMISSION FOR CLUSTER- BASED WIRELESS SENSOR NETWORKS IS INTRODUCED

J Karunamayi[1], Annapurna V K[2]

[1]*Student, Computer Network and Engineering,The National Institute of Engineering, Mysuru, Karnataka, (India)*

[2]*Associate Professor, Computer science and Engineering, The National Institute of Engineering, Mysuru, Karnataka, (India)*

ABSTRACT

Data forwarding in Wireless Sensor Networks, is insecure as wireless protocol provides least security measures. Clustering is an effective and practical way to enhance the system performance of WSN's. A study of secure data transmission for cluster-based WSN's is performed, where the clusters are formed dynamically. The 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 are proposed. The calculation results have been demonstrated to show the efficiency of proposed protocols in terms of minimization of energy consumption and security overhead.

Key Words: Cluster Based WSNs, CH, SN, SET-IBS, SET-IBOOS.

I. INTRODUCTION

Wireless Sensor Network (WSN) is a high and new technology consists of spatially distributed autonomous sensor nodes to monitor physical or environmental conditions such as sound, temperature, and motion. Wireless Sensor Networks take the advantage of deployment rapidly and strong survivability without fixed network support. WSNs also provide features of dynamic topology structure and limited energy resource and so on. One of the fundamental goals for Wireless Sensor Networks (WSNs) is to collect information from the physical world. Every node in WSNs are capable of sensing their environments, processing the data locally, and sending it to one or more collection points in a WSN. Efficient data transmission is one of the most important issues for WSNs. Meanwhile, many WSNs are deployed in neglected and 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.

1.1 Cluster Based Wireless Sensor Network

Clustering protocols are often used in sensor networks. In a cluster-based WSN (CWSN), every cluster has leader sensor node, regarded as cluster-head (CH). A CH aggregates the data collected by leaf nodes (non-CH sensor nodes) in its cluster, and sends the aggregation to the base station (BS) Cluster-based data transmission in WSNs has been investigated by researchers to achieve the networks scalability and management, which maximizes node life time and reduce bandwidth consumption. 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 BS is always reliable, the BS is 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 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. 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.

II. THE PROTOCOL OBJECTIVE

The goal of the proposed protocols for CWSNs is to:

- Create the secure and efficient data transmission for WSNs (CWSNs), where the clusters are formed dynamically and periodically.
- The SET-IBS and SET-IBOOS protocols need to consume energy faster than LEACH protocol because of the communication computational overhead for security either IBS or IBOOS process.
- The SET-IBOOS need to achieve a better balance of energy consumption than that of SecLEACH protocol.
- SET-IBS and SET-IBOOS protocols are to be implemented with respect to the security requirements.
- SET-IBS and SET-IBOOS protocols need to provide

➢ Authentication to the encrypted sensed data, by applying digital signature to the message packets.
➢ Solutions to passive attacks on wireless channel.
➢ Solutions to active attacks on wireless channel.
➢ Solutions to node compromising attacks.
➢ Solutions to orphan node problem.

III. SET - IDENTITY BASED DIGITAL SIGNATURE

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

3.1 Protocol Initialization

In SET-IBS, time is divided into successive time intervals, which are denoted by time-stamps T_s(for BS-to-node transmission) and T_i (for leaf-to-CH transmission). It is assumed that the BS

Adopt the node ID as it's public key under an IBS scheme for ID-based digital signature. The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. In this way, before a sensor node wants to authenticate itself to another node, it has to obtain its private key first. Because each private key is valid only during the current time interval, sensor nodes have to obtain a denotation of the new time interval to renew the private key at the beginning of a new round. Upon node revocation, the BS needs

to broadcast the compromised node IDs to the sensor nodes, each node stores the revoked IDs within the certain round. Additively adopt homomorphic encryption scheme to encrypt the plaintext of sensed data. This scheme allows efficient aggregation of encrypted data at the CHs and the BS, which also guarantees data confidentiality.

- 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*,G1,G2, *e*). Select a generator *P* of G1 stochastically.
- Choose two cryptographic hash functions: *H*, for point mapping hash function which maps strings to elements in G1, and *h*, for mapping arbitrary inputs to fixed-length outputs.
- Pick a random integer $\tau \in Z_t^*$ as the master key *msk*, set *Ppub*=τ *P* as network public key.
- Preload each sensor node with the system parameters $param_1$ = (*k*, *m*, *p*, *q*, E/F*p*,G1,G2, *e*, *H*, *h*, *P*, τ).

3.2 Key Management for Security

An SET-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 Phase: The BS (as a trust authority) generates a master key *msk* and public parameters *param* for the generation of private key and sends them to all sensor nodes.

Extraction Process: Node j first obtains its private key as from *msk* and its ID_j, where ID_j is the time stamp of node j's time interval in the current round that is generated by its CH i from the TDMA control.

Signature Signing: The sensor node j picks a random number and computes. The sensor node further computes

$cj = h(C_j \| t_j \| \theta_j)$ ---------- 1

$\sigma j = c_j\, sek_j + \alpha_j\, P$, ----------2

Where (σ_j, c_j) is the digital signature of node j on the encrypted message C_j. The broadcast message is now concatenated in the form of (IDj, t_j, C_j, σ_j, c_j)

Verification: Upon receiving the message, each sensor node verifies the authenticity in the following way. It checks the time stamp of current time interval t_j and determines whether the received message is fresh. Then, if the time stamp is correct, the sensor node further computes θ_j, = $e(\sigma_j,P)e(H(IDj \mid t_j, -p_{pub})c^j$ using the time stamp of current time interval . For authentication, 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.

3.3 Protocol Operation

SET-IBS operates in rounds during communication. Each round consists of a setup phase and a steady-state phase. All sensor nodes know the starting and ending time of each round because of the time synchronization. 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 TDMA control. Sensor nodes transmit the sensed data to the CHs in each frame of the steady-state phase. For fair energy consumption, nodes are randomly selected 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. 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 senor node becomes a CH for the current round. In the setup phase, the time stamp T_s and node ID_s are used for signature generation. Whereas in the steady-state phase, the time stamp t_j is used for the signature generation securing the inner cluster communications, and T_s is used for the signature securing the CH to BS data transmission.

3.4 Workflow of SET-IBS Protocol

Secure communication in SET-IBS relies on ID based cryptography in which user public keys are their ID information. Thus users can obtain their corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy. Fig 2 illustrates the process of encryption and decryption using the keys generated. As shown in fig private key is generated from nodes *ID* and mask (*msk*) function of the (BS). Similarly, public is generated from the *msk* function of CH. Using these keys security can be provided to the data.

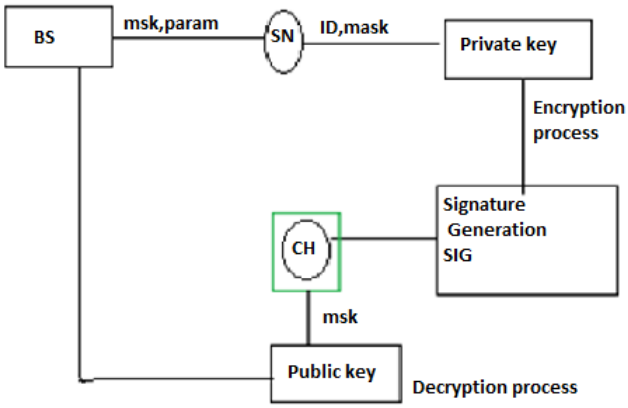

Fig 2: Workflow of SET-IBS Protocol

IV. SET - IDENTITY BASED ONLINE/OFFLINE DIGITAL SIGNATURE

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. The SET-IBOOS protocol is designed with the same purpose and scenarios for CWSNs with higher efficiency.

4.1 Protocol Initialization

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

- Generate an encryption key k for the homomorphic encryption scheme to encrypt data messages, where $k \in [m-1]$, m is a large integer.
- Let G be a multiplicative finite cyclic group with order q. The PKG selects a random generator g for group G generation, and chooses $x \in Z_q^*$ at random as the master secret key.

- Randomly select $r \in Z_q^*$ for each node private key generation, and let H be a hash function.
- Preload each sensor node with the public parameters, given by $param_2$= (k, m, G, q, g, x, r, H).

4.2 Key Management for Security

The IBOOS scheme in the proposed SET-IBOOS consists of following four operations: Setup phase, Key extraction, offline signing, online signing, and verification.

Setup Phase: The Base Station generates a master key *msk* and public parameter *param* for the generation of private key and sends them all to the sensor nodes.

Extraction Process: Before the signature process, node j first extracts the private key from the *msk* τ and its identity ID, as where

$$R_j = g_j^r$$

$$S_j = r_j + H(R_j, ID_j)\tau \ mod\ q.$$

Offline signing: At the offline stage, node j generates the offline value $< \sigma_j >$ with the time stamp of its time slot t_j for transmission, and store the knowledge for signing online signature when it sends the message. Notice that, this offline signature can be done by the sensor node itself or by the trustful third party, for example, the CH sensor node. Let then

$$g^{sj} = g^{rj\ gH(Rj, IDj)\tau mod\ q} = R_j\ X^{H(Rj, IDj)mod q}$$

$$\sigma_j = g^{-tj}$$

Online signing: At this stage, node j computes the online signature based on the encrypted data C_j and the offline Signature σ_j.

$$h_j = H(C_j, ID_j)$$

$$z_j = \sigma_j + h_j s_j \ mod\ q$$

$$\sigma_j = g^{\sigma\ j}$$

Then, node j sends the message to its destination with t_j ,R_j and the online signature, in the form of ID_j, t_j , R, σ_j, z_j , c_j .

Verification process: Upon receiving the message, each sensor node verifies the authenticity in the following way. It Checks the current time stamp t_j or freshness. Then, if the time stamp is correct, the sensor node further computes the Values of g^{zj} and $\sigma_j\ R_j\ h_j X^{\ hj\ H\ Rj\ ,\ IDj\ mod\ q}$,

If the values of and $\sigma_j\ R_j\ h_j X^{\ hj\ H\ Rj\ ,\ IDj\ mod\ q}$ are equal from the received message, the node i considers the received message authentic, accepts it, and propagates the message to the next hop or user. If the verification above fails, the sensor node considers the message as either a replaced one, or even a mistaken one, then ignores it.

4.3 Protocol Operation

The proposed SET-IBOOS operates similarly to that of SET-IBS. 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. However, the difference is that digital signatures are changed from the ID-based signatures to the online signatures (σ_j,Z_j) of the IBOOS scheme. Once the setup phase is over, the system turns into the steady-state phase, in which data are transmitted to the BS.

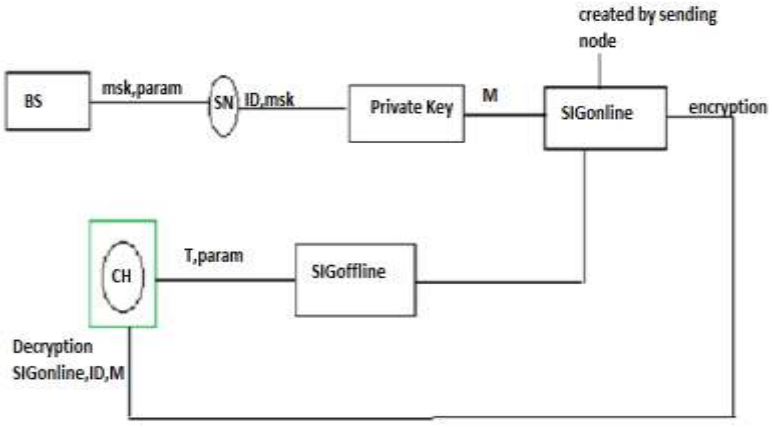

Fig 3: Workflow of SET-IBOOS Protocol

V. PROTOCOL FEATURES

The protocol characteristics and the features of the proposed SET-IBS and SET-IBOOS are as follows:

- Secure data transmission for CWSNs is provided by SET-IBS and SET-IBOOS protocols with concrete ID-based settings, which use ID information and digital signature for authentication
- Orphan-node problem in CWSNs is fully solved by the SET-IBS and SET-IBOOS schemes by using the symmetric key management.
- The secure and efficient data transmission protocol is ID based signature, uses the ID information and digital signature for verification in SET-IBS and SET-IBOOS scheme.
- The offline signature in SET-IBOOS 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.

VI. CONCLUSION

The deficiency of the symmetric key management for secure data transmission in CWSNs has overcome by the two secure and efficient data transmission protocols. Feasibility of SET-IBS and SET-IBOOS protocols with respect to the security requirements and analysis against routing attacks is discussed. By applying the ID-based crypto-system, SET-IBS and SET-IBOOS schemes are efficient in communication and achieves security requirements in CWSNs, also solves the orphan node problem with the asymmetric key management. Nodes lifetime, network scalability, and energy efficiency of CWSNs is improved by the performance of these protocols.

Secured data transmission in CWSNs is ensured by the SET-IBS and SET-IBOOS protocols.