ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 3, Issue 4, April 2015

Secure and Efficient Data Transmission in Cluster Based Wireless Sensor Networks using SET-IBS and SET-IBOOS Protocol

Biradar Arunabai

II Year M.Tech Scholar (CNE), Dept. of ISE, The Oxford College of Engineering, Bangalore, Karnataka, India

ABSTRACT: Efficient data transmission is an issue for wireless sensor networks. Efficient means providing security for data transmission and providing efficiency in data transmission for cluster based wireless sensor networks. Clustering is an effective way to enhance the system performance of wireless sensor networks. In this, the clusters are formed dynamically and periodically. The Identity based digital signature protocol is introduced in order to provide reliable data transmission for cluster-based wireless sensor networks. The Identity based digital signature protocol relies on the hardness of the Diffie-Hellman problem to provide security and also, identity based online-offline signature protocol introduced in order to avoid the security overhead in the identity based signature, identity based online-offline signature reduces the computational overhead of the protocol using discrete logarithm problem. This paper includes the feasibility of the protocol with respect to security requirements and security analysis over several attacks and deal with orphan node problem. The calculations and simulations are provided to illustrate the efficiency of the proposed protocol. The results show that, the proposed protocol have better performance than the existing secure protocols for cluster-based wireless sensor networks, in terms of security overhead and energy consumption.

KEYWORDS: CLUSTER-BASED WSNS, ID-BASED DIGITAL SIGNATURE, ID-BASED ONLINE/OFFLINE DIGITAL SIGNATURE, SECURE DATA TRANSMISSION PROTOCOL

I. INTRODUCTION

Due to the fast booming of micro electro mechanical systems, wireless sensor networking has been subject to extensive research efforts in recent years. It has been well recognized as a ubiquitous and general approach for some emerging applications such as environmental and habitat monitoring, surveillance and tracking for military. A wireless sensor network is usually composed of a large number of sensor nodes which are interconnected through wireless links to perform distributed sensing tasks. Each sensor node is low-cost but equipped with necessary sensing, data processing, and communicating components.

Therefore, when a sensor node generates a report after being triggered by a special event, e.g., a surrounding temperature change, it will send the report to a data collection unit (also known as *sink*) through an established routing path. Wireless sensor networks are usually deployed at unattended or hostile environments. Therefore, they are very vulnerable to various security attacks, such as selective forwarding, wormholes attacks. In addition, wireless sensor networks may also suffer from injecting false data attack.

For an injecting false data attack, an adversary first compromises several sensor nodes, accesses all keying materials stored in the compromised nodes, and then controls these compromised nodes to inject bogus information and send the false data to the *sink* to cause upper level error decision, as well as energy wasted in en-route nodes. For instance, an adversary could fabricate a wildfire event or report a wrong wildfire location information to the *sink*, then expensive resources will be wasted by sending rescue workers to a non-existing or wrong wildfire location. Therefore, it is crucial to filter the false data as accurately as possible in wireless sensor networks. At the same time, if all falsedata are flooding into

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

the *sink* simultaneously, then not only huge energy will be wasted in the en-route nodes, but also heavy verification burdens will undoubtedly.

II.RELATED WORK

The data transmission in WSNs can be done in two ways: (i) centralized (ii) decentralized. Centralized means such data processing and transfer can be carried out through or via the medium of a base station in WSNs .Whereas, in case of distributed or clustered wireless sensor environments, every cluster has obtained a high-configuration node called a cluster-head (CH). A sensor node of one cluster can only communicate with the other cluster‘s sensor node by taking the permission of the respective cluster. It is the function of cluster-head to aggregate all the data sent by sensor nodes.
[1] .Heinzelman *et al*. Proposed LEACH protocol is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. In order to prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensor nodes in the network, in rounds. LEACH achieves improvements in terms of network lifetime.

LEACH employs the following techniques to achieve the design goals stated:1) randomized, adaptive, self-configuring cluster formation; 2) localized control for data transfers; 3) low-energy media access control ; and 4) application-specific data processing, such as data aggregation or compression, protocol architecture where computation is performed locally to reduce the amount of transmitted data, network configuration and operation is done using local control, and media access control (MAC) and routing protocols enable low-energy networking, LEACH provides the high performance needed under the tight constraints of the wireless channel.

S-LEACH introduced a secure hierarchical protocol called S-LEACH, which is the secure version of LEACH. S-LEACH improves the method of electing cluster heads and forms dynamic stochastic multi-paths cluster heads chains to communicate to the base station, In this way it improve the energy-efficiency and hence prolong the lifetime of the network

[2] K. Zhang, C. Wang, and C. Wang introduced R-LEACH protocol, Secure solution for LEACH has been introduced called RLEACH in which cluster are formed dynamically and periodically. In RLEACH the orphan node problem is raised due to random pair-wise key scheme so they have used improved random pair-wise key scheme to overcome.

RLEACH has been used the one way hash chain, symmetric and asymmetric cryptography to provide security in the LEACH Hierarchical routing protocol. A hash chain is a method to produce many keys from a single key or password. For non-repudiation a hash function can be applied successively to additional pieces of data in order to record the chronology of data's existence.

RLEACH resists to many attack like spoofed, alter and replayed information, sinkhole, wormhole, selective forwarding, HELLO flooding and Sybil attack

[3] P. Banerjee, D. Jacobson, and S. Lahiri Introduced *Sec*-LEACH provides an efficient solution for securing communications in LEACH. It used random-key pre distribution and μTESLA for secure hierarchical WSN with dynamic cluster formation. Sec-LEACH applied random key distribution to LEACH, and introduced symmetric key and one way hash chain to provide confidentiality and freshness.

Sec-LEACH provides authenticity, integrity, confidentiality and freshness to communications, Key pre distribution is the method of distribution of keys onto nodes before deployment. Therefore, the nodes build up the network using their secret keys after deployment, that is, when they reach their target position. Key pre distribution schemes are various methods that have been developed by academicians for a better maintenance of key management in WSNs. Basically a key pre distribution scheme has 3 phases:

1. Key distribution
2. Shared key discovery
3. Path-key establishment

During these phases, secret keys are generated, placed in sensor nodes, and each sensor node searches the area in its communication range to find another node to communicate. A secure link is established when two nodes discover one or

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

more common keys, and communication is done on that link between those two nodes. Afterwards, paths are established connecting these links, to create a connected graph. The result is a wireless communication network functioning in its own way, according to the key pre distribution scheme used in creation. There are a number of aspects of WSNs on which key pre distribution schemes are competing to achieve a better result.

*[4]*Huang Lu *et.al* proposed a new secure routing protocol with ID-based signature scheme for cluster-based WSNs within which the security is dependent on the hardness of the Diffie-Hellman problem in the random oracle model. Here the deficiency in the secure routing protocols with symmetric key pairing is pointed out by authors. Because of the communicationOperating cost for security, authors provide simulation investigation results in details to demonstrate how various parameters act among energy efficiency and security as in [4].

[5] Pantazis *et.al* presented a classification of energy efficient routing protocols and expanded the classification initially done by Al-Kariki to better describe which issues/operations in each protocol illustrate/enhance the energy efficiency issues.

The distributed behavior and dynamic topology of Wireless Sensor Networks (WSNs) brings in many unusual requirements in routing protocols that should be fulfilled. The main important aspect of a routing protocol, so as to be efficient for WSNs, is the energy usage and the extension of the network's life span. During the past few years, a lot of energy efficient routing protocols have been projected for WSNs.

The authors here presented the four types of schemes of energy efficient routing protocols: Network Structure, Communication Model, Topology Based and Reliable Routing. The routing protocols which belong to the first type can be additionally classified as hierarchical or flat. The routing protocols belonging to the second type can be additionally classified as Query-based or Coherent and non-coherent based or Negotiation-based. The routing protocols belonging to the third type can be additionally classified as Location-based or Mobile Agent-based. The routing protocols belonging to the fourth type can be additionally classified as QoS-based or Multipath based. Lastly, a systematic review on energy efficient routing protocols for WSNs is provided as in.

[6] Pairing for IBS: Boneh and Franklin introduced the first functional and efficient ID-based encryption scheme based on bilinear pairings on elliptic curves. Specifically, randomly select two large primes p and q, and let E/Fp indicate an elliptic curve $y2 = x3 + ax + b$ ($4a3 + 27b2 \_ 0$) over a finite field Fp. We denote by G1 a q-order subgroup of the additive group of points in E/Fp, and G2 a q-order subgroup of the multiplicative group in the finite field F$*p$. The pairing is a mapping e G1×G1→G2, which is a bilinear map with the following properties.

1) *Bilinear*: $\forall P, Q, R, S \in$G1, $e(P + Q, R + S) = e(P, R)\, e(P, S) e(Q, R)\, e(Q, S)$. In the same way, $\forall c, d \in Z*q$, $e(cP, dQ) = e(P, dQ)\, c = e(cP, Q)\, d = e(P, Q)\, cd$, etc.

2) *Non-degeneracy*: If P is a generator of G1, then $e(P, P)$ is a generator of G2.

3) *Computability*: There is an efficient algorithm to compute (P, Q) in G_2, $\forall P, Q \in G_1$.

The security in the IBS scheme is based on the bilinear Diffie-Hellman Problem (DHP) in the pairing domain,

And the hardness of DHP is defined in .A bilinear map e is secure if, given $g, G, H \in G_1$, it is hard to find $h \in G_1$ such that $e(h, H) = e(g, G)$. Weil pairing [6] and Tate pairing are the examples of such bilinear mapping, which present comprehensive descriptions of how pairing parameters can be selected for security.

III. PROPOSED SYSTEM

We are proposing two secure and efficient data transmission protocol called as SET-IBS and SET-IBOOS, in order to reduce the security overhead in SET-IBS we are proposing SET-IBOOS, these are based on IBOOS and IBS schemes.

Architecture diagram

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 3, Issue 4, April 2015

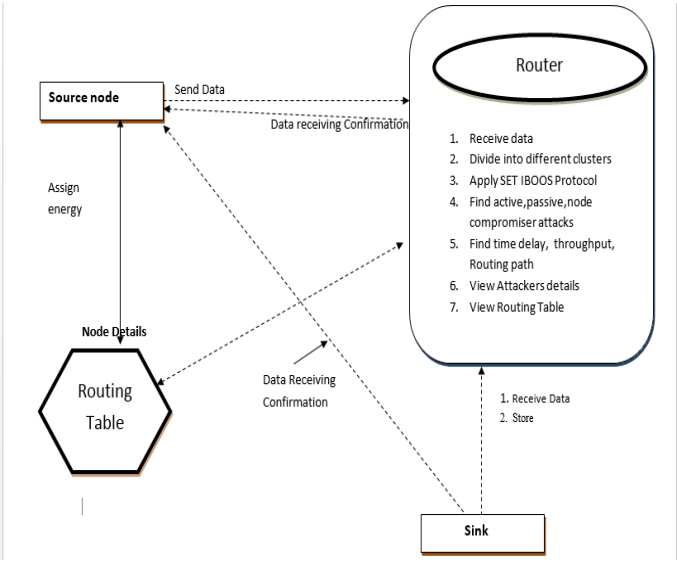

Fig 1: Architecture Diagram

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. 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

SET-IBS SCHEME

The proposed SET-IBS has a protocol initialization prior to the network deployment and operates in rounds during communication, which consists of a setup phase and a steady-state phase in each round.

1. Protocol initialization

In SET-IBS, time is divided into successive time intervals. Time-stamps are denoted by *Ts* for BS-to-node communication and by *ti* for leaf-to-CH communication. The key pre-distribution is an efficient method to improve communication security. 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. The homomorphic encryption scheme to encrypt the plaintext of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 3, Issue 4, April 2015

sensed data. This scheme allows efficient aggregation of encrypted data at the CHs and the BS, which also guarantees data confidentiality.

2. Key management for security

The sensor node *j* transmits a message *M*, andencrypts the data using the encryption key *k* from the additively homomorphic encryption scheme. We denote the cipher text of the encrypted message as *C*. In order to adapt the algorithms of IBS to WSNs practically, we simplify the mapping *e* with one generator *P* and provide the full algorithm in the signature verification. The IBS scheme in the proposed SET-IBS consists of following three operations,extraction, signing and verification.

3. Protocol operation

After the protocol initialization, SET-IBS operates in rounds during communication. Each round consists of a setup phase and a steady-state phase. We suppose that, all sensor nodes know the starting and ending time of each round, because of the time synchronization. The operation of SET-IBS is divided by rounds 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. 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 .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.

SET-IBOOS SCHEME

Theproposed SET-IBOOS operates similarly to the previous SETIBS, which has a protocol initialization prior to the network deployment and operates in rounds during communication.

1. Protocol initialization

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.

2. Key management for security

IBOOS scheme based onthe DLP in the multiplicativegroup, and propose a novel secure data transmissionprotocol 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 proposedSET-IBOOS consists of following four operations, extraction, offline signing, online signing andverification.

Extraction*:* Before the signature process, it first extracts Private keys from the master secret key *x* and its identity *ID*, as $sek=(R, s_i)$, where

$$R = g_r,$$

$$s_i = r + H(R, ID_i)\, x \bmod q.$$

Offline signing*:* It generates the offline signature $\sigma i$with the time-stamp of its time slot t_i for transmission, and store the knowledge for signing online signature when it sends the message. Notice that, this offline signature can be done by the sensor node itself or by the trustful third party, e.g., the BS or the CH sensor node.

Let $X = g_x$, then,

$$g_{s_i} = g_r g_{H(R, ID_i)\, x \bmod q} = RX_{H(R, ID_i) \bmod q}.$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 3, Issue 4, April 2015

$\sigma_i = g^{-t_i}$.

Online signing*:* At this stage, node A_i computes the online signature σ_i, z_i based on the encrypted data C and the offline signature σ_i.

$h_i = H(C||\sigma_i)$.

$z_i = \sigma_i + h_i s_i \bmod q$,

$\sigma_i = g^{\sigma_i}$.

Then node A_i sends the encrypted message to its destination with the signature $\_ID_i$, σ_i, z_i, C.

Verification*:* Upon receiving the message, each sensor node verifies the authenticity in the following way. It checks the current time-stamp t_i for freshness. Then, if the time-stamp is correct, the sensor node further computes the value of gziand $\sigma_i R^{h_i} X^{h_i H(R,ID_i)} \bmod q$ using the online signature $\_\sigma_i, z_i\_$, then check if

$g^{z_i?} = \sigma_i R^{h_i} X^{h_i H(R,ID_i)} \bmod q$.

For correctness, we have the equation at the CH node as shown below.

$$\sigma_i R^{h_i} X^{h_i H(R, IDi)} \bmod q$$
$$= g^{\sigma_i} g^{r h_i} g^{x h_i H(R, IDi)} \bmod q$$
$$= g^{\sigma_i + h_i (r + (H(R, IDi) x \bmod q))}$$
$$= g^{\sigma_i + h_i s_i \bmod q} = g^{z_i}.$$

If it is equal to the equation above in the received message, the sensor node 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 messages either bogus or a replaced one, even a mistaken one, then rejects or ignores it

3. 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.

IV.CONCLUSION

In this paper, it is reviewed that the data transmission issues and the security issues in cluster based wireless networks. The deficiency of the symmetric key management for secure data transmission has been discussed. It is then presented two secure and efficient data transmission protocols respectively for cluster based wireless networks, reliable data transmission identity based digital signature protocol. In the evaluation section, it is provided feasibility of the proposed efficient data transmission identity based digital signature protocol with respect to the security requirements and analysis against routing attacks. reliable data transmission identity based digital signature protocol is efficient in communication and applying the ID-based crypto-system, which achieves security requirements in cluster based wireless networks, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management.

REFERENCES

1. 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.
2. 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
3.P. Banerjee, D. Jacobson, and S. Lahiri, "Security and performance analysis of a secure clustering protocol for sensor networks," in *Proc. IEEE NCA*, 2007.
4. Huang Lu, Jie Li, Kameda, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID-Based Digital Signature" in H.Global Telecommunications Conference (GLOBECOM 2010), Page(s): 1- 5, Publication Year: 2010.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

5. D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," in *Lect. Notes. Comput. Sc. - CRYPTO*, 2001
6. D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," in *Lect. Notes. Comput. Sc. - CRYPTO*, 2001.
7 J. Liu and J. Zhou, "An Efficient Identity-Based Online/Offline Encryption Scheme," in *Lect. Notes. Comput. Sc. - Appl. Crypto. Netw. Secur.*, 2009

BIOGRAPHY

Ms. Biradar Arunabai a Student of Information Science and Engineering Department at The Oxford College of Engineering-Bangalore, affiliated to VTU pursuing M.Tech in Computer Networking and Engineering. She received her Bachelors of Engineering in Computer science and Engineering from Rural Engineering College Bhalki affiliated to VTU**.** Her research interests are Wireless Sensor Networks and information security.