Identity Based Online / Offline Digital Signature Scheme in Cluster Based Wireless Sensor Networks for Secure and Efficient Data Transmission

Kanchana.R[1], Yamini.G[2]
[1, 2] Department of Computer Science and Engineering
[1, 2] Bharathidasan University, Trichy

Abstract- *In the past few years high secure network transmission data along with efficiency is a different critical issue for Wireless Sensor Networks (WSNs). Clustering is an effectively and conventional way to enhance performance of the WSN system. In this research we study a secure transmission of network data for cluster-based WSNs (CWSNs), where the clusters are organized dynamically and sporadically. We make use of Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBOOS, by means of the Identity-Based Online/Offline digital Signature (IBOOS) scheme, correspondingly. The proposed system relies on the hardness of the Differ-Hellman problem in the pairing area in SET-IBOOS scheme and it reduces the operating cost in protocol security using SET-IBOOS scheme, which is critical for WSNs.*

I. INTRODUCTION

Network Based on information technology, a network is a series of points or nodes interconnected by communication paths. Networks can also be interconnect with other networks and may contain sub networks. A group of interconnected computers and peripherals either by using wire like cable and wireless is capable of sharing software and hardware resources between many users.

Low Energy Adaptive Clustering Hierarchy ("LEACH") is a TDMA-based MAC protocol which is integrated with clustering and a simple routing protocol in wireless sensor networks (WSNs). The goal Of LEACH is to lower the energy consumption required to create and maintain clusters in order to improve the life time of a wireless sensor network. LEACH In a cluster-based WSN (CWSN), every cluster has a leader sensor node, regarded as cluster head (CH). A CH aggregates the data collected by the leaf nodes (non-CH sensor nodes) in its cluster, and sends the aggregation to the base station (BS). The low-energy adaptive clustering hierarchy (LEACH) protocol presented is a widely known and effective one to reduce and balance the total energy consumption for CWSNs.To prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensors nodes in the network, in rounds. LEACH achieves improvements in terms of network lifetime.

The feasibility of the asymmetric key management has been used 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 IBOOS scheme has been proposed to reduce the computation and storage costs of signature processing. A general method for constructing online/offline signature schemes was introduced. The IBOOS scheme could be effective for the key management in WSNs. Specifically; the offline phase can be executed on a sensor node or at the BS prior to communication, while the online phase is to be executed during communication.

Background

In [1] key exchange is a big overhead for any secure data transmission protocols. This is removed in the proposed system by introducing Base Station. SET-IBOOS Scheme reduces the computational overhead

In [2] The survey show that the SET-IBS SET-IBOOS protocols have better performance than the existing LEACH , LEACH LIKE PROTOCOLS for CWSNs, in terms of security overhead and energy consumption.

In [3] the comparison in the calculation and simulation results show that, the proposed SET-IBS and SETIBOOS 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 SETIBOOS with less auxiliary security.

In [4] their simulation results show that Enhanced LEACH outperformed LEACH in terms of the network lifetime and balanced energy consumption.

II. METHODOLOGY

This system has one base station. The purpose of the base station is to provide common key parameters to all the nodes in the system. Every node in the system can form their encryption key by following notations.

Node ID + Common Parameter For each transaction base station creates new common parameter, so that for every transaction new key is generated.

This system has two routing protocols. SET-IBS & SET-IBOOS

III. SET-IBOOS

Base station has the option to select which protocol to be applied during transmitting the data.

SET-IBOOS While source node is sending a message to the destination, it has to create identity based digital signature by using Hashing technique and encryption technique, this is called Online Signature. This is sent to cluster head. The first cluster head once it receives the message has to take its current time of received message. Then it has to take MAC value and append the value along with the message and forward the message to routing cluster head. Routing cluster head has to forward message to destination cluster head. The final cluster head has to check whether the message is reached within the correct time or not. Time delay attack is detected by checking the MAC value generated by its system current time. Once destination node receives the message, it has to decrypt the Online Signature and get Message Authentication Code (MAC 1).It has to create MAC 2 using Hashing technique from message. It has to compare MAC 1 and MAC 2. If both are same then it has to accept the message otherwise it has to reject the message.

Problem implementation phases

SET Protocol

a. Key management for security
b. Neighborhood authentication
c. Storage cost
d. Network scalability
e. Communication overhead
f. Computational overhead
g. Attack resilience

IV. EXPERIMENTAL RESULTS

Method to improve performance of WSN data Transfer

To improve the efficiency in the SET IBOOS protocol, the improved SET-IBOOS protocol is proposed which the online/offline attribute based encryption method is used.

Setup phase: The setup algorithm takes as input a security parameter λ and a universe description U, which defines the set of allowed attributes in the system. It outputs the public parameters PK and the master secret key MK.

Extraction process: The extract algorithm takes as input the master secret key MK and an access structure (resp., set of attributes) $Ikey$ and outputs a private key SK associated with the attributes. Offline. Encrypt (PK): The offline encryption algorithm takes as input the public parameters PK and outputs an intermediate cipher text IT. Online. Encrypt (PK, IT,: The online encryption algorithm takes as input the public parameters PK, an intermediate cipher text IT and a set of attributes (resp., access structure) and outputs a session key and a cipher text CT. Decrypt (SK; CT) → key.

The decryption algorithm takes as input a private key SK for $Ikey$ and a cipher text CT associated with) $Ienc$ and encapsulates cipher text CT to recover a session key

The core part of the system is the base station. Base station provides common key parameters to all the nodes in the system.

Each node in the system can frame the encryption key by following notations.

Node_ ID + Common_ Parameter The base station creates new common parameter for each transaction.

Therefore for each transaction new key is generated.

The System Architecture is shown in the Fig1.

Workflow of SET-IBOOS and its Operation SET-IBOOS is proposed in order to further reduce the computational overhead for security using the IBOOS scheme, in which security relies on the hardness of the discrete logarithmic problem.Private key is generated in similar way as that of IBS, Along with private key online signature is generated for encrypting the data. This online signature is obtained using offline signature. While decrypting the data online signature, sensor node ID and message M parameters

are used.

V. WORKING MODULE DESCRIPTION

Module use the system is divided into the following modules.

- Base Station
- Senders Source
- Cluster Head
- Routing Cluster
- Head Destination
- Cluster Head

Attacker Receivers

1) **Base Station** The base station controls the entire system. The base station consists of two phases-Setup phase and Steady State phase. The base station generates the master key pairs with the help of Encryption Algorithm. These keys are unique to each other. In the set up status the keys are generated. In the steady state keys are sent to corresponding nodes. The nodes all are identified by its own identity.

2) **Senders** the sender is one of the end user. The sender sends the data through the network with cryptographic mode. The sender encrypts the message by using Encryption technique and obtains the MAC value for the message.

The sender will send the encrypted message along with MAC value.

3) Before the message is forwarded it will take its own time stamp and is concatenated with the message. It is then forwarded to the routing cluster head.

4) **Routing Cluster** Head In the routing cluster the attacker module is located. There are two types of attacker module: Content change attacker module and Time delay attacker module. The routing cluster forward the data to the destination cluster in the form of packets.

5) **Attacker module** there are two types of attacker module: Content change attacker module and Time delay attacker module. The time delay attacker delays the data transferring rate. The content change attacker changes the content of the data content.

6) **Destination Cluster** Headthe destination cluster head checks the data arrival time with its own system time. If it reaches more than its threshold time limit, then the delay has occurred resulting in time delay attack. If it reaches before the threshold time the data is forwarded to the corresponding node.

7) **Receivers**The receiver is one of the end user. The receiver receives the data from the destination cluster head. The data is checked whether it is corrupted or not. The received data is decrypted by the help of Decryption Technique and the MAC is obtained. This is compared with the sender's MAC. If it matches the message is not corrupted. The message is accepted by the receiver. Otherwise the message is rejected which is attacked by the attacker module.

VI. PROTOCOLS USED

The source node sends a message to the destination. The identity based digital signature is created for the message. This is done using encryption technique and MD5 Hashing technique. This is termed as Online Signature. This is sent to the source cluster head. The source cluster head once it receives the message has to takes the current time of message received. Then it takes the MAC value and appends it along with the message. This is then forwarded to the routing cluster head. Routing cluster forwards the message to destination cluster head. The destination cluster head checks arrival time of the message. It then checks whether it reaches within the given time limit or not. The time-delay-attack is detected. This is performed by detecting the MAC value generated by the current time of the system. Once it receives the message, it decrypts the Online Signature and gets MAC1.The node in the destination creates MAC2 from the message using MD5 Hashing technique. It compares MAC2 with MAC1. If it matches, the message is accepted. Otherwise the message is rejected.

V. PROTOCOL FEATURES

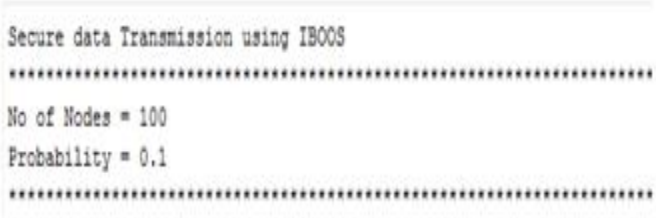

Fig 1 Simulation Node Details

The protocols SET IBOOS are used for transmission of data effectively in a secure manner.

A. PROTOCOL CHARACTERISTICS

Key Management: Asymmetric based cryptographies are used for key management.

Overhead in communication: The overhead in the data packets during communication is less.

Cost of storage: The amount of memory required for the security keys in sensor node is less

Table 1 Parameter Value

Network Field	100 × 100 m
(Number of Nodes)	100
Intitial Energy	1 J
Elec(E.Dissipation for ETx & ERx)	50 n /bit
εfs(free space)	10 pJ/bit/
εmp(Multipath fading)	0.0013 pJ/bit/
EDA(Energy Aggregation Data)	5 nJ/bit/signal
Esig	77.4 µJ/signature
Eoff	5 µJ/signature
Eon	12.37 µJ/signature
Data Packet Size	4000 bits
Tool used for implementation	MATLAB 7.6.0

```
Secure data Transmission using IBOOS
************************************************
No of Nodes = 100
Probability = 0.1
************************************************
Intialize Energy = 0.5
************************************************
Transfer Energy = 5e-008
************************************************
Recieve Energy = 5e-008
************************************************
```

Fig 2 Simulation Energy Details

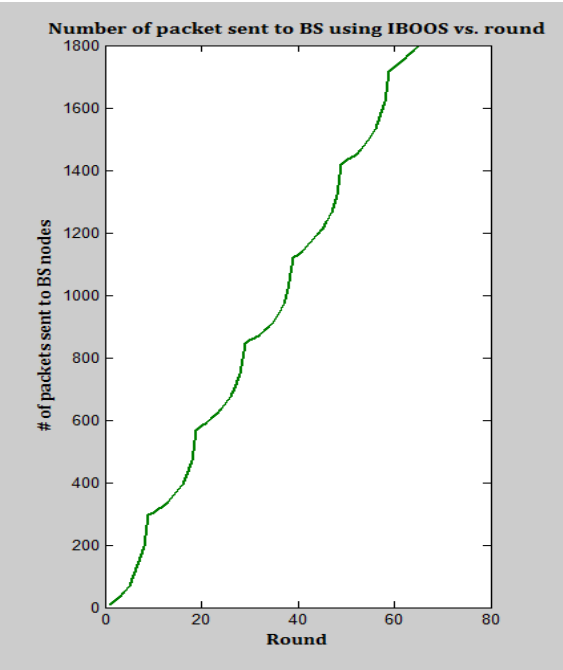

Fig 3 Number of packet sent to BS using IBOOS

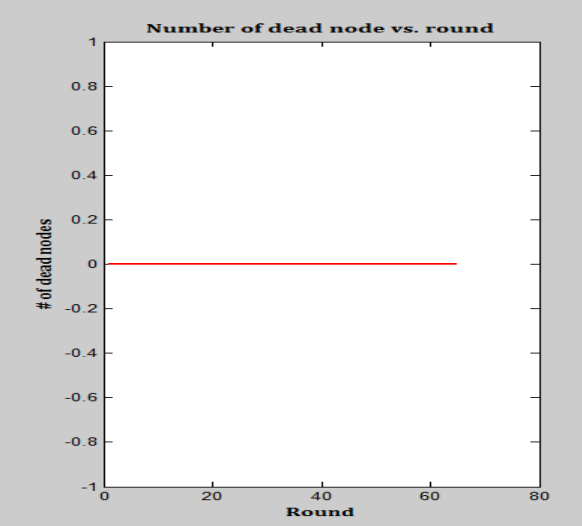

Fig 4 No of Dead Nodes

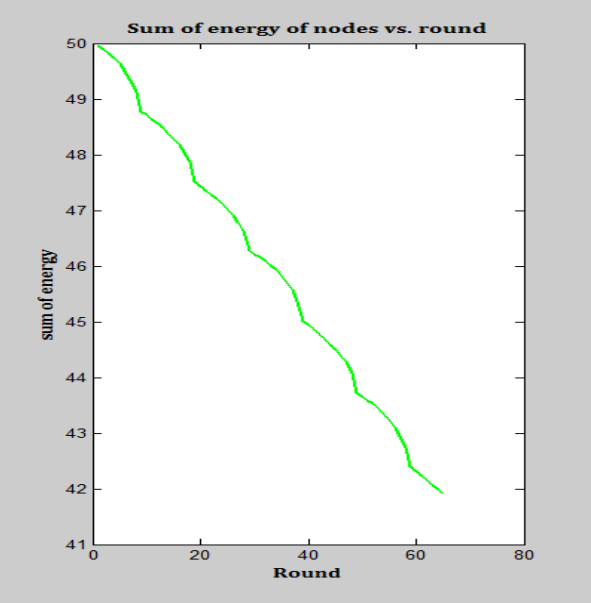

Fig5.5 Sum of the Enegy of nodes

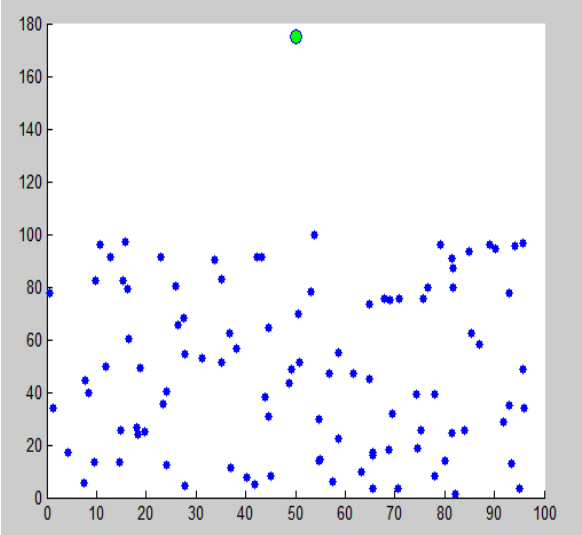

Fig 5 Simulation Environment

VI. RESULTS AND DISCUSSION

1. Initially, base station is centralized and 100 nodes are setup in a particular region (100 x 100) and each node has equal energy (0.5 joules).

2. In round 1, Cluster Head will be created according to probability condition.

3. The decision of each node to become cluster head is taken based on the suggested percentage of cluster head nodes p. 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 cluster-head for the current round. The threshold value is calculated based on an equation that incorporates the desired percentage to become a cluster-head, the current round, and the set of nodes that have not been selected as a cluster-head in the last (1/p) rounds, denoted by G. T (n) is given by:
   And, for IBS and IBOOS, the cluster head selection formula is:

   Where, Ecru is current energy of a particular node and Einitis initial energy of a particular node.

   Optimal number of cluster heads is estimated to be 10% of the total number of nodes.

4. Then, Nodes sends the data to their respective cluster heads and energy consumption will be calculated.

   Energy calculation for Nodes in LEACH-C:

   WHERE, d0 is given by:√ ⁄ Energy calculation for Nodes in IBS:

5. Cluster Head will aggregate the data and send it to the base station and energy consumption will be calculated for each node and cluster heads.

   Energy calculation for Cluster Head in LEACH-C and IBS:

   If (dis > d0)
   (ETX+ EDA)*(d) + Emp*d*(min_dis4) (9)
   If (dis<= d0)
   (ETX+ EDA)*(d) + Efs*d*(min_dis2) (10)

   Energy calculation for Nodes in IBOOS:

6. In round 2, the nodes will become cluster heads according to probability conditionT (n).

7. After selection of cluster heads, Nodes sends the data to their respective cluster heads, that will be selected according to the minimum distance of a particular node from cluster heads and energy consumption will be calculated.

8. Cluster Head will aggregate the data and send it to the base station and energy consumption will be calculated.

9. This process will be repeated until the whole network gets down or number of rounds finished.

10. Performance will be evaluated according to parameters like network lifetime, energy dissipation, no. of data packets sent etc.

VII. CONCLUSION

The limited availability of energy on network nodes is one of the critical issue in wsn this paper increases network lifetime and increase the efficiency in the performance of routing protocols. In hierarchical routing architecture, sensor nodes self-configure themselves for the formation of cluster heads that cluster head is used to send data packets from or to the main base station. This paper is to design a routing protocol which is secure and energy was conserved.

REFERENCES

[1] Two new secure and efficient data transmission protocols SET-IBS and SETIBOOS for wsn international journal of innovative research in computer and communication engineering roshima. P.p, ramakrishna.m, k.n. Narasimha murthy 2015

[2] Identity based digital signature scheme in cluster based wireless sensor networks for secure and efficient data transmission – a survey,muthusamy sc.poongodi ,ijaict journal, at coimbatore 2014

[3] Enhancement of secure and efficient data transmission in cluster based wireless sensor networks nagesh babu v, arudra.a international journal of scientific and research publications, volume 4, issue 6, June 2014

[4] Enhanced leach protocol for wireless sensor networks a.koucheryavy,ahmedsalim, and walid osamy 2014

[5] 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.

[6] J S Rauthan, S Mishra" An Improved Approach in Clustering Algorithm for Load Balancing in Wireless Sensor Networks "International Journal of Advanced Research in Computer Engineering & Technology, July 2012

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

[8] P.Banerjee,D.Jacobson,andS.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.

[9] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," Proc. Fourth Int'l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM), pp. 1-5, 2008

[10] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in Proceedings of the 33rd Annual Hawaii International Conference on System Siences (HICSS '33), p. 223, January 2000