Id-Based Signature For Energy Efficient WSN

Ms. Roshani R. Patle, Dept. of Computer Engineering, Smt.Kashibai Navale College of Engineering, Vadgaon, Pune, India Phone +91-8378990765

Mrs. Rachana Satao, Dept. of Computer Engineering, Smt.Kashibai Navale College of Engineering, Vadgaon, Pune, India Phone +91-9405009877

***Abstract*— in wireless sensor network (WSN) transmission of data securely is a critical issue. Clustering is powerful and feasible way to improve performance of the WSN system. We study transmission of data securely for clustered WSNs (CWSNs). We use two Secure and Efficient data Transmission (SET) protocols for CWSNs called SET-IBS and SET-IBOOS. SET-IBS uses the Identity-Based digital Signature (IBS) scheme and SET-IBOOS uses Identity-Based Online/Offline digital Signature (IBOOS) scheme. In SET-IBS security depends on the hardness of Diffie-Hellman problem in the pairing region. SET-IBOOS diminishes the operating cost of computation for protocol security, which is important for WSN, while its defense depends on durability of problem of discrete logarithm. Cluster head selection and clustering are important in WSN to route data efficiently. Multi Weight Based Clustering Algorithm (MWBCA) is an extended LEACH where cluster head is elected on weight given to each sensor node. We used Multi Weight Based Clustering Algorithm (MWBCA) for Cluster Head selection, then aggregate data at cluster head and going to provide security using Identity based Digital Signature.**

***Index Terms*—CWSN, ID-based digital signature, ID-based online/offline digital signature, SET.**

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a network system which consist of spatially distributed devices like wireless sensor nodes. These sensor nodes monitor physical or environmental conditions like sound, temperature and motion. The individual node are able to sense their environment, processing the data locally and sending data collectively to one or more collection points in a WSN(BS).

In sensor network very important aspect is the flow of data. It contains information which may be important for some application. So there should be a secure data transmission. But maintaining security is difficult for sensor nodes because they have limited energy and limited memory capacity. Reports are made from the data received from sensor nodes. These report must be authenticate and reach without modification to the Base station.WSN are used in many application like military, ecological and health related area. This application may be surrounded by harsh, neglected and often adversarial physical environment. So Secure and Efficient data transmission (SET) is necessary and is important issue in WSN.

Researchers invented Cluster-based data transmission in WSN (CWSN) to achieve network scalability and management. This maximizes lifespan of nodes and reduces consumption of bandwidth among sensor nodes. CWSN contain cluster of sensor nodes from which one of them is selected as Cluster Head (CH). Data collected by leaf node (non-CH sensor nodes) is aggregated at CH and send it to the base station (BS).

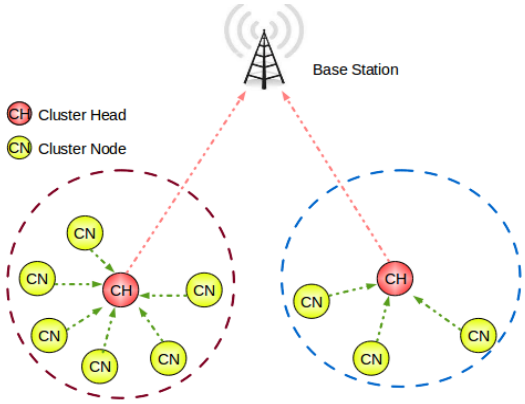

Fig 1.Clustered WSN

II. MOTIVATION

Wireless Sensor Networks (WSNs) are used in many applications in military, ecological, and health-related areas. These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in a building. Security is therefore important in WSNs. However, WSNs suffer from many constraints, including low computation capability, small memory, limited energy resources, susceptibility to physical capture, and the use of insecure wireless communication channels.

The low –energy adaptive clustering hierarchy (LEACH) [2] is widely known protocol in CWSN. Adding security to LEACH- like protocol is challenging because they dynamically, randomly and periodically rearrange the network's cluster and data link. Therefore, providing steady long-lasting node-to-node trust relationships and common key distributions are inadequate for LEACH-like protocols. There are some secure data transmission protocols based on LEACH-like protocols, such as SecLEACH [4], RLEACH [6]. Most of them, however, apply the symmetric key management for security, which suffers from a so-called orphan node problem. This problem occurs when a node does

not share a pairwise key with others in its preloaded key ring. It cannot participate in any cluster, and therefore, has to elect itself as a CH. Furthermore, the orphan node problem increases the overhead of transmission and system energy consumption by raising the number of CHs.

The feasibility of the asymmetric key management has been shown in WSNs recently, which compensate 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. Here digital signature is used for the binding between public key and identification of signer. Identity based digital signature scheme is based on difficulty of factoring integers from identity based Cryptography. In this entity's public key is derived from its identity information like its name or ID number. Recently the concept of IBS has been developed as a key management in WSN for security.

III. STATE OF ART

Security is very important aspect in WSN. Different types of attacks are possible in the data transmission in WSN. Many protocols are investigated for providing security to clustered WSN.

Y. Wang, G. Attebury [1] has described communication architecture, constraint, security requirement and threat models of WSN. According to security requirement attacks are classified. Most of the security issues in WSN are solved by cryptography. So selecting appropriate cryptographic technique is important in WSN. Author discussed public key cryptography and symmetric key cryptography in this paper. W. Heinzelman, A. Chandrakasan [2] has designed protocol for micro-sensor network. First he studied various parameters relevant to sensor application and then introduced LEACH protocol architecture. In LEACH local clusters are formed among nodes. Energy load of being cluster head is balanced among the nodes. Then author has suggested LEACH-C protocol. Protocol uses centralized clustering algorithm and steady state protocol like LEACH. LEACH-C produce better cluster than LEACH because BS (Base Station) has knowledge about location and energy of all nodes in the network.

L.B. Oliveira et al [4] has considered clusters which are formed dynamically and periodically in hierarchical (cluster based) sensor networks. Adding security to these networks is very difficult. To address the security, author has investigated random key pre-distribution and μTESLA building block from SPINS. It provides secure communication. Author has proposed SecLEACH protocol.

P. Banerjee, D. Jacobson, and S. Lahiri [5] have proposed new protocol GS-LEACH for CWSN. Main idea of this protocol is based on LEACH. It optimizes consumption of energy and provides secure communication to the network of different shapes. It uses Grid based deployment. Author compared various parameters of GS-LEACH with LEACH and SecLEACH like energy consumption, different shapes of deployment area, security analysis. GS-LEACH protocol outperforms LEACH and SecLEACH.

K. Zhang, C. Wang, and C. Wang [6] have proposed R-LEACH protocol for CWSN. It is advanced version of LEACH provides secure communication between member nodes and CH by random pair wise key scheme. This scheme depends on the probability of connection between sensor nodes. It provides authorization of nodes which is used to solve many security issues. This protocol provides security from various attacks like selective forwarding, Sybil and hello flood attack. In this way it improves secure communication between nodes.

H. Lu, J. Li, and H. Kameda [12] have studied secure routing for CWSN where clusters are formed dynamically and periodically. For CWSN he proposed secure routing protocol using ID-based digital signature where ID-based cryptography is used. ID-based digital signature security depends on the hardness of Diffie-Hellman problem. Proposed protocol provides confidentiality, authenticity, non-repudiation, integrity and freshness to the communication between sensor nodes. It also provides protection against certain attacks like sinkhole, hello flood and selective forwarding.

Huang Lu, Jie Li, and Mohsen Guizani, [13] has proposed two protocols, SET-IBS and SET-IBOOS for secure and efficient transmission of data in CWSN. SET-IBS is Secure and Efficient Identity based scheme and SET-IBOOS is Secure and Efficient Identity based Online/Offline scheme. These schemes provide security against various attacks.

IV. MATHEMATICAL MODEL

1. Sensor Network.
   Sensor network consisting of N sensor, we denote that the i-th sensor by Si and the corresponding node set by
   v= {v1, v2, vN,}, |v |=N},
   Set of communication links
   E= {e1 ، e2 ، ⋯ ، eN),
   Suppose that V is always connected.

2. Neighbor.
   For any node whose neighbor node set are defined as follows:
   $Vi = \{i \in N | d(Vi, Vj) \leq R, n \neq i\}$,
   Where,
   N - The collection of all nodes
   d (Vi, Vj) - the distance between node Vi, and Vj,
   R - Broadcasting range of nodes.

3. The energy spent for transmission of a k-bit packet over distance d is:
   $E_{Tx}(k, d) = k * E_{elec} + k * \varepsilon_{fs} * d^2 \quad d < d_0 \quad (1)$
   $= k * E_{elec} + k * \varepsilon_{mp} * d^4 \quad d >= d_0 \quad (2)$
   Where,
   E_{elec} - base energy required to run the transmitter or receiver circuitry
   ε_{fs} & ε_{mp} – Energy of the transmitter amplifier
   To receive the message energy required is
   $E_{RX}(k) = k * E_{elec} \quad (3)$

4. Elliptical curve digital signature scheme
   There are curve parameters (CURVE, G, n)
   CURVE – The elliptical curve
   G – Elliptical curve base point, a generator of the elliptical curve with large prime order n.
   n – Integer order of G

4.1 Key Generation

Sensor node creates a key pair,

Private key integer d_A, randomly selected in the interval [1, n-1]

public key curve point $Q_A = d_A . G$.

4.2. Signature signing algorithm

1. Calculate e = HASH (m)
2. Let z be the L_n leftmost bits of e, where L_n is the bit length of the group order n.
3. Select a cryptographically secure random integer k from [1, n-1].
4. Calculate the curve point $(x_1 , y_1) = k . G.$ (4)
5. Calculate $r = x_1 \bmod n.$ (5)

If r = 0, go back to step 3.

6. Calculate $s = k\text{-}1(z + r . dA) \bmod n.$ (6)

If s = 0, go back to step 3.

7. The signature is the pair (r, s).

4.3. Signature verification algorithm

1. Verify that r and s are integers in [1, n-1]. If not, the signature is invalid.
2. Calculate e = HASH (m),
3. Let z be the L_n leftmost bits of e. (7)
4. Calculate $w = s^{-1} \bmod n.$ (8)
5. Calculate $u_1 = z . w \bmod n$ and $u_2 = r . w \bmod n.$ (9)
6. Calculate the curve point $(x_1 , y_1) = u_1 \times G + u_2 \times Q_A$ (10)
7. The signature is valid if $r = x_1 \bmod n$, invalid otherwise.

V. PROPOSED METHOD

Identity based Signature for WSN is used to achieve following objective-

- Reduce energy consumption than LEACH protocol.
- Provide security to clustered WSN by avoiding denial-of-service attack.

In the proposed system clustering and digital signature is implemented for balancing the load on cluster head in clustered WSN. We are considering to providing security to Multi-weight Based Clustering Algorithm (MWBCA). In MWBCA cluster head is elected by considering many factors like,

- Residual energy,
- Cluster head time count,
- Number of neighbor nodes.

MWBCA is used in order to reduce energy limitation and imbalance energy consumption in sensor nodes. In clustered WSN achieving secure and efficient data transmission from cluster nodes to CH is very important. Existing system is implemented on LEACH protocol where cluster head are selected randomly. In my proposed system I am going to use MWBCA which effectively balance energy consumption and provide security in data transmission by using Identity Based Digital Signature scheme.

Digital Signature employs a type of asymmetric cryptography. For message sent through a non-secure channel properly implemented digital signature gives the receiver reason to believe the message was sent by claimed sender.

Following are the steps in the design phase for secure transmission of data between cluster node and CH.

1. Base station broadcast its information with its Master key.
2. Sensor node decides to become a CH for current round based on max of $P_{Vi\text{-}ch}$ value

$$P_{Vi\text{-}ch} = \alpha * \deg(v_i) + \beta * (E_{vi\_current} / E_{vi\_max}) + \gamma (1/ T (V)) \quad (11)$$

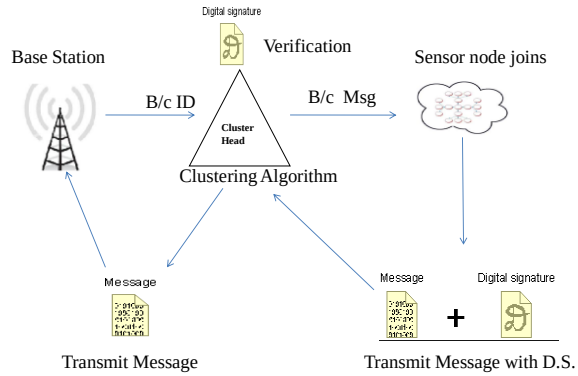

Fig 2: System architecture

Where,

deg (vi) = number of neighbor node of vi

$E_{vi\_current}$ =current energy of node vi

E_{vi_max} = initial energy of node vi

T (V) = elected time of CHvi

α, β and γ = weighting factor

1. CH broadcast advertisement message (adv) to the neighboring nodes
2. Cluster node picks CH with largest received signal strength of adv message and joins to CH
3. Leaf sensor node transmits data to the CH with digital signature. After verification data will get transmitted to CH. During verification we check security of data. Each CH collects message from all members and and aggregate data.
4. CH sends aggregated data to the BS.

Proposed system contains two modules –

1. Clustering Algorithm
2. Digital signature Scheme

1. Clustering Algorithm

We will model the wireless sensor networks. It is assumed that the nature of network is as follow:

(1) All of nodes are homogeneous .Each node has certain amount of initial energy E · Each node is assigned a unique identifier (ID).

(2) It consists of a BS, away from the nodes deployed in a square filed, through which the end user can access data from the sensor network.

Description of MWBCA -

All nodes should be alternately take turns to become CH, in order to prevent early death due to excessive energy expenditure. Nodes with higher residual energy should be

selected as cluster-head than the nodes with low-energy. CH election needs to consider following factors,
(1) Residual energy- Since the initial energy of each node is the same. If the node's residual energy is greater than it represent the energy consumed is less. So that node is more suitable is selected as the CH to balance the network energy consumption.
(2) Cluster head time count - All nodes should have a responsibility to become as CH. Therefore, if CH has less time then it is more suitable to be selected as cluster head.
(3)The number of neighbors. Neighbor nodes are used to check amount of information transmitted and energy consumption.

Considering the above three factors, the weight of node can be calculated by eq. (11) Node with the largest $P_{Vi\text{-}ch}$ value is selected as a cluster head

2. Elliptical Curve Digital Signature Algorithm
There are curve parameters (CURVE, G, n)

CURVE – The elliptical curve

G – Elliptical curve base point, a generator of the elliptical curve with large prime order n.

n – Integer order of G

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. It contains following steps –

1. Key Generation

Sensor node creates a key pair, consisting of a private key integer d_A, randomly selected in the interval [1, n-1] public key curve point $Q_A = d_A . G$.

2. Signature signing algorithm

Given message M, Digital signature is created by sensor node.

3. Signature verification

At CH digital signature is verified. If signature is valid then only message will get accepted otherwise rejected.

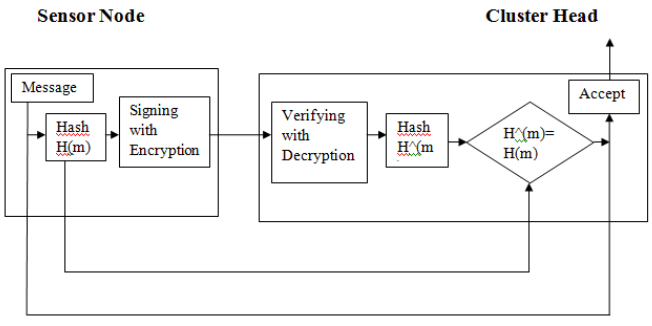

Fig 3. Signing and Verification of Messages

Simulation and Result –

Here JUNG simulator is used for the implementation of project.

Consider CWSN which contain fixed BS and many sensor nodes. Sensor nodes are grouped into clusters and each cluster has CH node. Data will be transmitted from sensor node to CH and then aggregated data will be transmitted to BS.

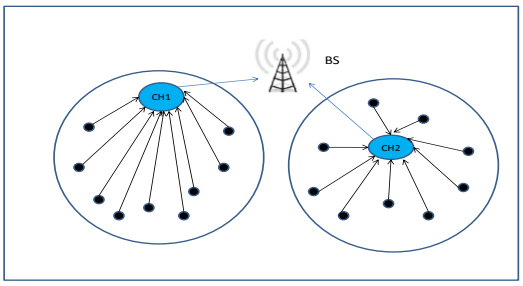

Fig 4. Network architecture

Following are the steps during implementation of project –

- We select number of nodes dynamically and Base Station is fixed
- Then we are doing data transmission using LEACH
  1. Clusters are formed
  2. Public key and private key is created for each sensor node.
  3. Public key are exchanged.
  4. While sending data to the BS digital signature is created and verified at the CH and then data will be transmitted to the BS.
- Then we are doing data transmission using MWBCA

Steps 1 to 4 are repeated again.
At the end energy consumed by LEACH and MWBCA are compared.

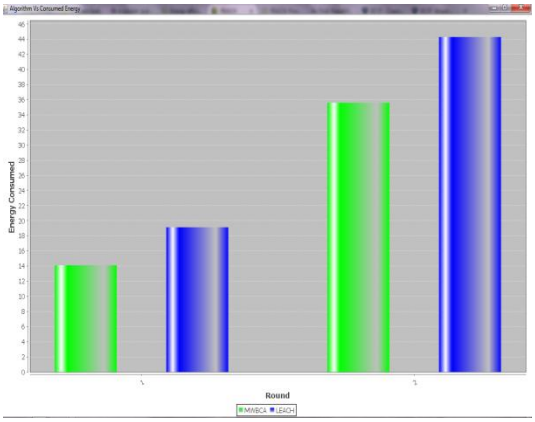

Fig. 5 Energy consumption in MWBCA and LEACH

We can see from fig.5 that energy consumed using MWBCA is less than LEACH.
We can see from fig. 6 that number of packet loss in MWBCA is less than LEACH.

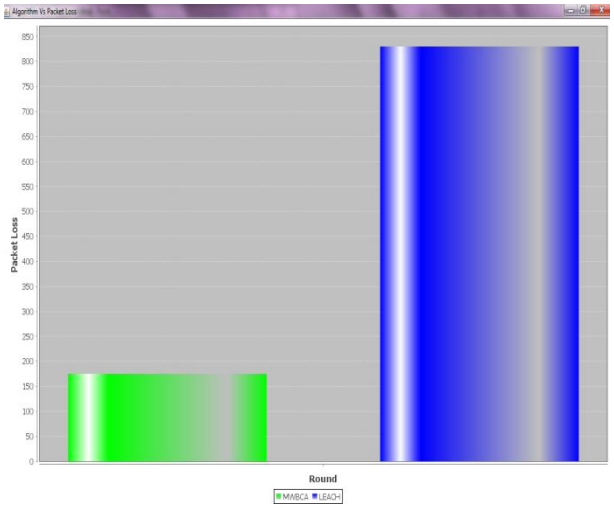

Fig. 6 Packet loss in MWBCA and LEACH

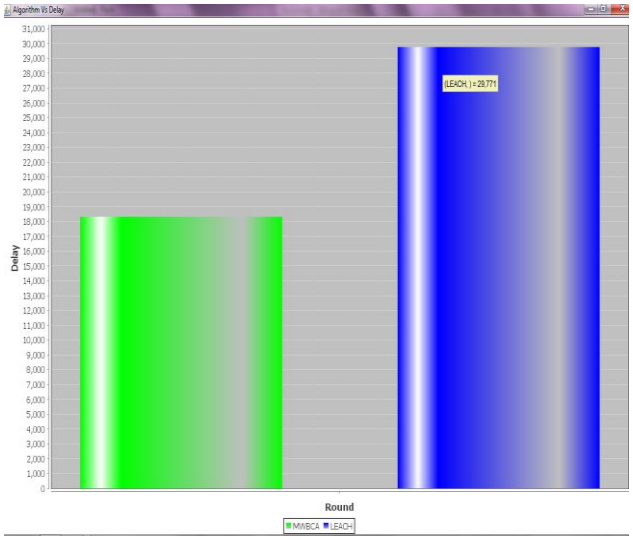

Fig. 7 Packet Delay in MWBCA and LEACH

We can see from fig. 7 that packet Delay in MWBCA is less than LEACH.

Applying security to clustered WSN – Secure data transmission will be achieving using Digital Signature. In this we are going to provide security for the transmission of data between sensor node and cluster head by avoiding denial of service attack.

VI. CONCLUSION

In this paper for secure data transmission we first identified various secure protocols used in the CWSN which uses symmetric key management and studied various identity based schemes. Then we studied IBOOS scheme. Routing algorithm in sensor network is a very hot research topic because it saves energy and prolong network lifetime. Multiweight based Clustering Algorithm balances energy effectively than LEACH. We are going to provide security to Multi Weight based cluster in CWSN. Multi weight based clustering is used for energy balancing in network and Identity Based Digital Signature is used to provide security in the data transmission in CWSN against Denial of Service attack. It is worth noting that proposed method will reduce energy consumption in clustered WSN.

Our proposed method can also be extended for a two level hierarchical clustered WSN. In which security can be provided by applying digital signature between Cluster Head and Base station.

REFERENCES

[1] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Comm. Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.

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

[3] A.Manjeshwar, Q.-A. Zeng, and D.P. Agrawal, "An Analytical Model for Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," IEEE Trans. Parallel &Distributed Systems, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.

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

[5] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks," Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA), pp. 145-152, 2007.

[6] 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.

[7] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, vol. IT-22, no. 6, pp. 644-654, Nov.1976.

[8] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Proc. Advances in Cryptology (CRYPTO), pp. 47-53, 1985.

[9] D.W. Carman, "New Directions in Sensor Network Key Management," Int'l J. Distributed Sensor Networks, vol. 1, pp. 3-15, 2005.

[10] R. Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks Using Identity-Based Signatures," Proc. IEEE Int'l Conf. Computer and Information Technology (CIT), pp. 882-889, 2010.

[11] H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID-Based Digital Signature," Proc. IEEE GLOBECOM, pp. 1-5, 2010.

[12] Huang Lu, Jie Li, and Mohsen Guizani, "Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks" IEEE Trans. Parallel &Distributed Systems,vol. 25, no. 3, March 2014

[13] Zhiping FAN, Zhengzhe JIN," A Multi-weight Based Clustering Algorithm for Wireless Sensor Networks" PRZEGLĄD ELEKTROTECHNICZNY (Electrical Review), 2012

