ISSN (Print) : 2319-8613
ISSN (Online) : 0975-4024

Security Enhancement using Chaotic Map and Secure Encryption Transmission for Wireless Sensor Networks

R.Santhosh[#], M.Shalini[*]

[#]Assistant Professor, Department of Computer Science and Engineering,
Karpagam University, Coimbatore, India
santhoshrd@gmail.com

[*]PG Scholar, Department of Computer Science and Engineering,
Karpagam University, Coimbatore, India
shalinisiet@gmail.com

***Abstract*--Wireless Sensor Network (WSN) is a collection of variety of sensor nodes. Wireless sensor network allures the researchers with its research procedures and it is applied on various sites. Based on chaotic map and genetic operations, a lightweight block cipher is implemented to address these limitations. Elliptic curve points and one of the chaotic map parameters are employed in this cryptographic scheme to verify the communicating nodes and also output the bit sequence pseudo randomly. To encrypt the data blocks, XOR, mutation and crossover operations are used in this sequence. Chaotic map and genetic operations is mechanism used in sensor networks to provide confidentiality and security for data. In addition to Chaotic map algorithm, secure encryption transaction algorithms are used to verify the nodes by checking whether it is transferred by Authorized user or not. In future this protocol is used for audio and video encryption.**

Keyword- WSN, Set-IBS, Set-IBOOS

I. INTRODUCTION

Wireless sensor network (WSN) also known as Wireless Sensor and Actuator Network (WSAN) are spatious sensor collection which is distributed autonomously for guarding conditions of physical and environmental. It passes the data over the sensor nodes to main network cooperatively. Thereby enabling control of sensor activity, the more contemporary networks are said to be bi-directional. The WSN consist of variety of nodes where every node is combined with one or more sensor nodes.

To transfer the messages from normal sensor nodes to the Base Station (BS), cluster heads are responsible. Communication can be done easily between the base station and cluster heads, that can be found anywhere in the network and changes per definite length of time and also improves network's energy ratio. In spite of functioning of dimensions of microscopic size that have to be created, nodes of sensors may differ in size. Sensor node's size and economic limitations result in restrictions of needed resources like bandwidth, memory, speed and energy.

Key management often receives more concern in authentication and encryption of data in wireless sensor network. Due to the limitations of resources in wireless sensor networks, Diffie-Hellman and RSA public key based algorithms are more difficult and consumption of energy is high in WSN.

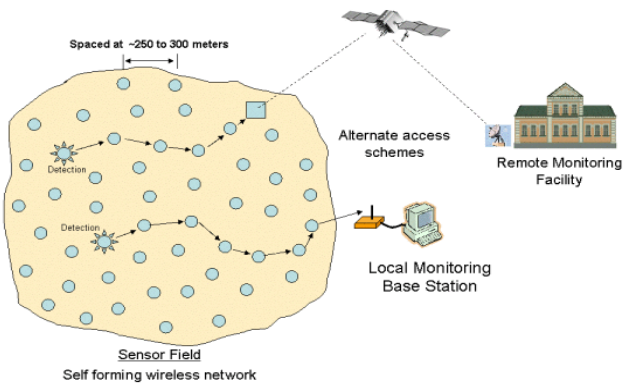

Fig. 1. Sensor Network Architecture

When compared to public key cryptography for WSN, the symmetric techniques of cryptography consist of own value which makes highly efficient. Sensor nodes must accomplish keys for encryption in order to provide security in WSN. The delivery of variety of keys over nodes of sensor device is referred as key distribution.

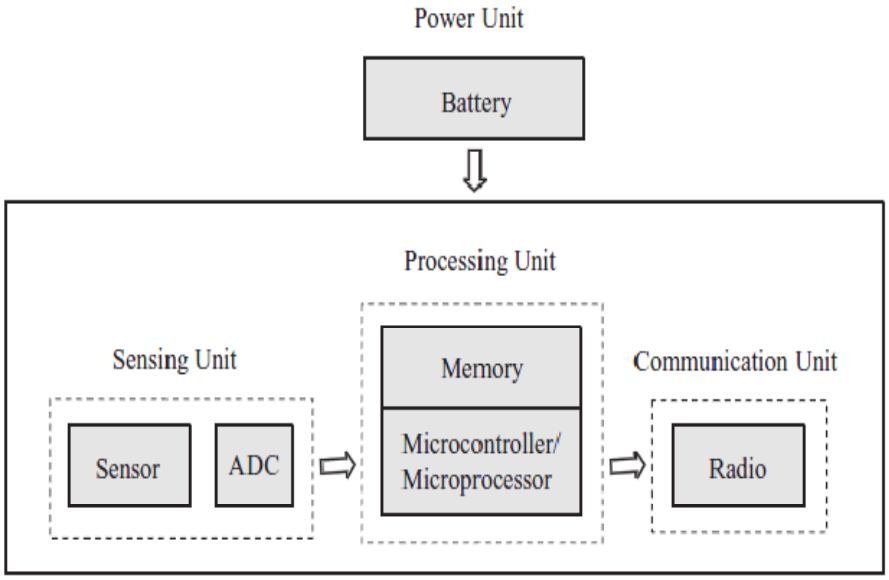

Fig. 2. Architecture of Sensor Node

II. RELATED WORK

Number of security attacks are exposed to the transmission protocols of data which also includes cluster-oriented protocols are exposed to a [12][14]. The algorithms used are classified into three classifications for security purpose. They are conventional block cipher and lightweight block cipher and hardware based compact cryptographic schemes. Cluster head attacks in WSNs results in severe harm to the network instead out sending and aggregation of information fundamentally that depends on the cluster heads. If a hacker handles to act like attacks of selective forwarding, thereby it promotes attacks similar sink hole and damaging the network.

The present research on security is focused on design of lightweight block cipher which is more secure. Inspite of the researchers activity, most of the cryptographic schemes which is conventional is compared in which lightweight ciphers which have relatively worst execution. In order to address these limitations, cipher block based to genetic operations of chaotic map was introduced in sensor network devices combining both sender and receiver nodes which is small that enables less cost and data communication securely.

III. PROPOSED SYSTEM

The proposed system aims to guarantee the data transmissions to be secure and efficient between nodes existing intermediately. The existing algorithms for encryption process tend to use key management technique for security purpose. This causes many issues. With the help of chaotic map algorithm and secure encryption techniques we try to correct those issues thereby reducing computational overhead in Secure and Efficient data Transmission- Identity Based digital Signature (SET-IBS) with the help of IBOOS scheme.

A. Network Module

In the network, nodes of sensors are located uniquely. In an undirected graph G, the nodes are connected with edges that are communicated with each other. In the graph V and E are represented in which V denotes the collection of vertices that denotes the network node set and E denotes the number of edges that denotes the travelling path location of moving nodes. Consider N as a network of travelling nodes denoted as s. N1, N2...Ns are the collection of nodes delivered in the network where 1 to s types of nodes are there. Considering any two mobile nodes *Ni* and *Nj*, delay in transmission of a data is represented as *Tij.* Delay is represented in unit-size that is transferred to those two nodes.

B. Bit Sequence

Bit sequence phase produces bit sequences using the algorithms chosen. The test code is used to decide the randomness of the binary sequence derived [15]. Chaotic maps algorithm involves floating point calculation to generate the random numbers continuously. They are not suited for wireless sensor networks consisting of limited resources. Chaotic map discretely influences security level which relies on never ending period and unpredictability properties of random number generation technique. Using logistic map of N frequencies provides advantage of handling the parameters which is of integer points that limits the wireless sensor

network's operational computing process. The equations followed explain the chaotic functions which derive the bit sequences in the scheme implemented.

$$xn + 1 = \mu xn(N - xn/m)/N - yn/2 \quad (1)$$

$$yn + 1 = \beta(N - |N - yn|) \quad (2)$$

Where,

$$x \in (0, m \times N), \mu \in [0, 4], y \in (0, 2 \times N),$$
$$\beta \in [4, 5],$$

$N = 2K$ and $m = 2k$ *with* K and k as integers. Used key holding values of s, N, μ, and β are pre distributed in the sensor nodes which includes set consisting of values {xi , yi , m, N, μ, β} and the key establishment phase are exchanged with the initial values of xi and yi.

C. Encryption Phase

There are two principles used namely confusion and diffusion to shape the block cipher pattern. Confusion technique is the communication among the symmetric key with cipher text. Diffusion is assuming the duplicacy of the plaintext. XOR, mutation and crossover are the three operations used for the proposed scheme. *XOR* denotes the xor operation applied between the bit that is longer than the plaintext. The technique of considering bit strings of two parent bits and predicting the bit strings of corresponding child is referred as *Crossover* operation. This operation exchanges the bit string's parts between the parents. The process of combining the strings in the bits is referred as *Mutation*. In the cipher text, the diffusion and confusion properties are achieved with the help of mutation and crossover genetic operations. After completing the mutation operation the order of the image data and text data are changed with the help of crossover operation. A fair difference in cipher text is the advantage of using genetic operations proceeding to plaintext.

D. Network Clustering

Fig 3. Shows the clustering network which consist of base station, cluster head and mobile nodes where functionalities and capabilities are homogenous in nature. The nodes of sensor may be convinced by hackers and on wireless channel, the transmission of data may be disturbed by attacks. In clustering network, group of clusters are developed by sensor nodes in which every clusters has a CH(Cluster Head). Depending on the signal strength received, clustered sensor node without cluster head is joined and the data sensed is transmitted through CH to the BS to save energy. Base station is always authentic. It implies that the base station is a confidential authority. The CHs transmit data to the BS directly thus performing data fusion and with comparatively high energy.

In wireless sensor networks, sensing of data, processing of data and transmission of data influences

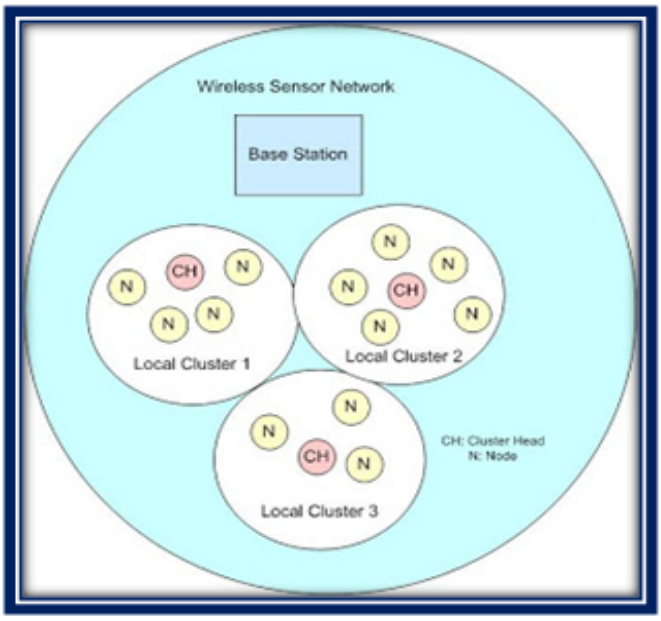

Fig 3. Clustering Network

sensor node's energy consumption. The cost incurred in transmitting data is more costly. TDMA referred as Time Division Multiple Access control is used to send data. Thus, the node present in the middle of network

(e.g., a CH) collects and combines the needed information and send back it to the base station which is better than the method in which information is received by the base station directly sent by the sensor node [16][19]. Along with that, all sensor nodes are assumed in which the BS are coordinated with time along with corresponding radio frequency channels. The energy is constrained in which the nodes are distributed randomly. When sensor node presents idle without sensing or transmitting data, it changes into sleeping mode to save energy.

E . SET-IBS

Operations on pre-distribution of key to the nodes of sensor networks are performed by the base station. The Identity Based digital Signature scheme in the developed SET-IBS algorithm comprised of three different operations. They are signing, verification and extraction techniques. Extraction node first obtains the private key of the node. Then the generated time stamp by the channel head of a node's time interval in the current round from the TDMA control is also obtained. A random number is chosen by the sensor node and computed generation with the help of Signature signing. In Verification, authenticity is verified by each sensor node in the corresponding way upon receiving the message. After initialising the protocol, during communication SET-IBS operates in rounds. To encrypt data messages for similar encryption scheme the base station generates an encryption key k, where I is the huge integer. Considering equities,

$$\text{Equi}=\{k, m, n, p, q, E/F, G1, G2, H, h, \tau, P\}$$

generator P of G1 is selected practically. Point mapping hash function denoting H and arbitrary input mapping h are two cryptographic hash functions. In G1, H points elements as strings and h points to fixed-length outputs.

- An integer is chosen randomly as the master key mk , *Ppub=p* is set as public key of the network.
- Every node of sensor network should be preloaded along the equities of the system. $\{k, m, n, p, q, E/F, G1, G2, H, h, \tau, P\}$
- A leaf sensor node i is assumed to send a message M to its cluster head j and the data is encrypted with the help of encryption key k from homomorphic encryption scheme.

The node of sensor network i selects a number randomly i=>q and computes i = E(p,P). The encrypted message's cipher text is denoted as Extraction node denoted as i first get *pki* as its private key from *mk* and *IDEj*, where *IDEj* is its identity, and ti refers the time stamp of node I that is produced by its cluster head j as time gap in the present round from the TDMA control. Then the computation of sensor node network is denoted as

$$cj = (h/\ cj\ //tj//\theta j) \quad (1)$$

$$\sigma j = cj\ sekj + \alpha j\ P \quad (2)$$

Where $(\sigma j, cj)$ denote the encrypted message *Cj*.'s digital signature node i. After receiving the message the broadcast message is then combined in which each sensor node verifies the time interval's time stamp and confirms the legal nodes and thereby checks that the received message is clean. The sensor node checks whether the received message is authorized or not. The sensor node with the help of the current time gap ti's time stamp is evaluated, if the time stamp is right. Then the message is moved to the next hop or user. The message is considered by the sensor node as either attacked or restored, if the verification fails. Although it can be a defected one and it ignores that. Then the stage starts and during communication SET-IBS operates in rounds.

F. SET-IBOOS

This phase generates the identity based online offline digital signature method. For distribution of key in the network, the following operation is done by the base station. For the homomorphic encryption scheme, exhibit an encryption key k for data messages encoding process, where *k=>(*N-1), N is considered as huge integer. A random generator g of group CG generation is chosen by the public key generator and also t=>*Zq** is chosen as the master key *mk* at random**.** A multiplicative finite cyclic group is denoted as CG with order q. For its private key production randomly select *ri=>Zq** for each and every node i.

G. Performance Evaluation

Many experiments are conducted for validation of proposed algorithms. Assumption of the uniform distribution of nodes is applied in this experiment, in the sensing field. For sink in small and large networks, the relative network behavior, throughput, overhead and lifetime is compared to cover the uncovered node using relay node. According to the number of nodes, Fig 4. represents the comparison of sender and receiver networks behavior. Fig 5. Shows the increase in data packets delivery issue considering throughput and overhead, Fig 6. illustrates the increase in lifetime of sensor network nodes.

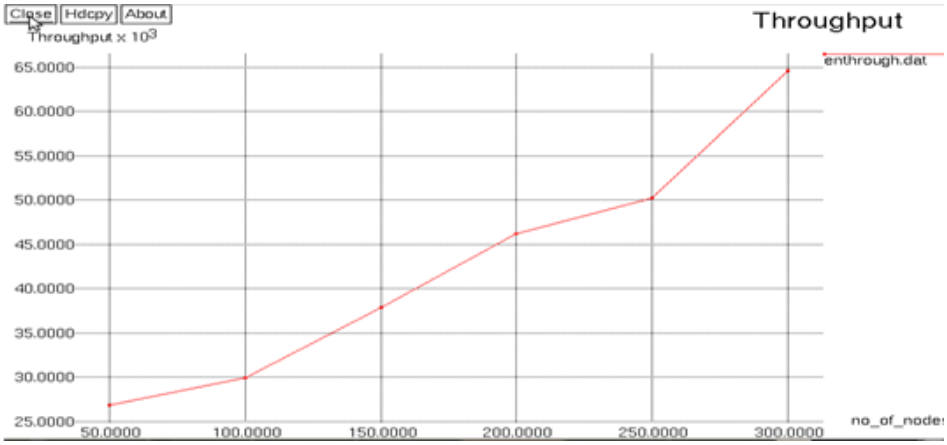

Fig 4. Network Behavior

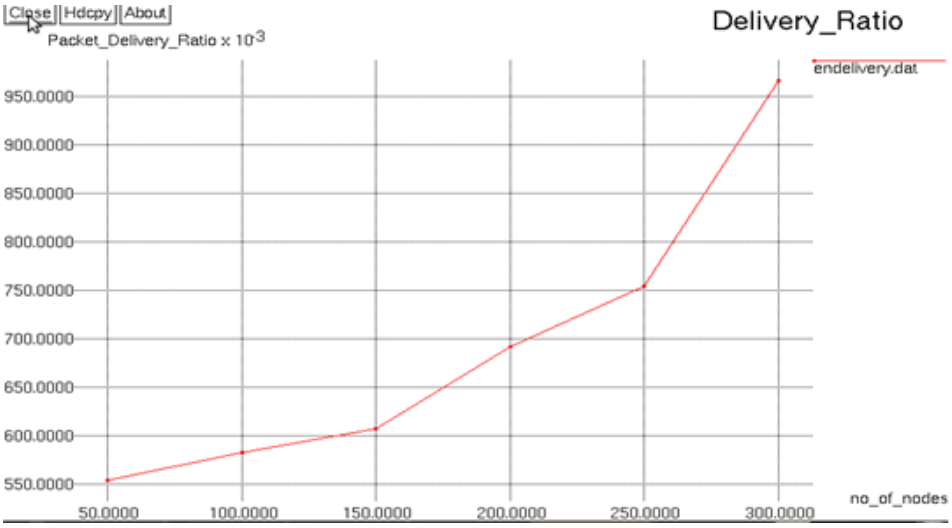

Fig 5. Data Packets Delivery Issue

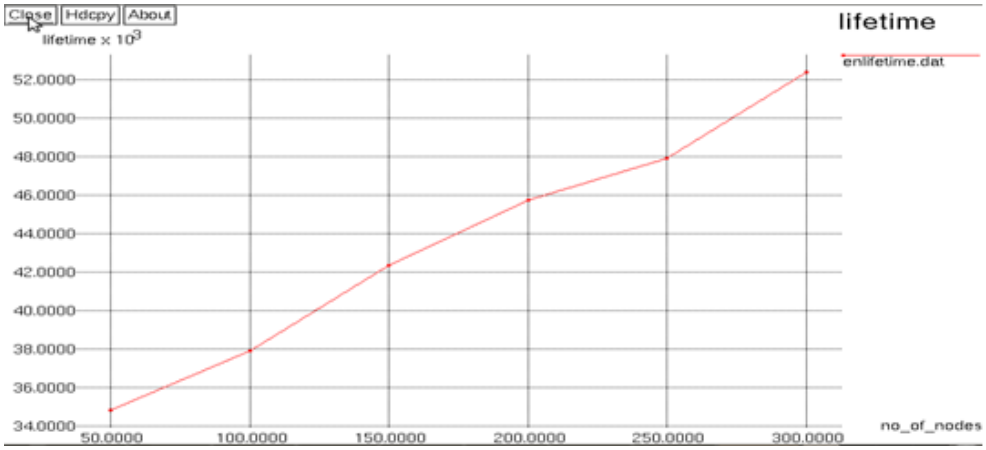

Fig 6. Lifetime of Sensor Network Nodes

IV. CONCLUSION

Issues related to transmission of data and security in wireless sensor network is first reviewed. After that transmission protocols for WSN are used which is secure and more efficient? The protocols used are chaotic map and genetic operations, secure encryption transmission protocols based on IBS and IBOOS scheme. For transmission of data securely, the disadvantages of the symmetric key management is discussed. The performance of the implemented schemes of SET-IBS and SET-IBOOS algorithms were analyzed in this evaluation. Routing attack analysis and security requirements were evaluated. The algorithms used are more efficient to communicate. Identity based cryptosystem is accomplished for security requirements in sensor

networks. By using SET-IBOOS scheme, with respect to network costs associated, security overhead is minimized which is needed for secure data transmission in wireless sensor networks.

REFERENCES

[1] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures".
[2] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures".
[3] I. Ituen and G. Sohn, "The Environmental Applications of Wireless Sensor Networks".
[4] G. W. Allen, K. Lorinca, M. Welsh, O. Marcillo, J. Johnson, M. Ruiz, and J. Lees, "Deploying a Wireless Sensor Network on an Active Volcano".
[5] Dr.D.Sivakumar, S.Srikiran Rao, S.Gokula Krishnan, V.Guru Karthikeyan, "Case Study: Setting up VOIP Network Over Wireless Mesh Network in Campus".
[6] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, J. Anderson, "Wireless Sensor Networks for Habitat Monitoring".
[7] Vineeta Philip, Pratikkumar Bharti, Ketankumar Dorik, Aishwarya Venkatesh , Munazza Farha Arshi, "UWB Ad- Hoc Wireless Sensor Network for Structural Health Monitoring and Facility Management of Warehouses".
[8] K. Pradeepa, W.R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks".
[9] Anthony Rowe, Dhiraj Goel, Raj Rajkumar "FireFly Mosaic: A VisionEnabled Wireless Sensor Networking System".
[10] E. Sazonov, K. Janoyan, and R. Jha, "Wireless Intelligent Sensor Network for Autonomous Structural Health Monitoring".
[11] L.B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks," Signal Processing".
[12] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing".
[13] D.W. Carman, "New Directions in Sensor Network Key Management".
[14] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks".
[15] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures".
[16] T. Hara, V.I. Zadorozhny, and E. Buchmann, "Wireless Sensor Network Technologies for the Information Explosion Era".
[17] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks".
[18] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks".
[19] A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks".
[20] J. Liu et al., "Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network," Int'l J. Information Security".
[21] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security".
[22] S. Sharma and S.K. Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks".
[23] A. Manjeshwar, Q.-A. Zeng, and D.P. Agrawal, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol".

AUTHOR PROFILE

Dr.R.Santhosh received his B.Tech degree in Information Technology from K.S.R College of Technology in 2006, M.E degree in Software Engineering from Sri Ramakrishna Engineering College in 2009, M.B.A in Education Management from Alagappa University in 2011 and Ph.D in Computer Science and Engineering at Karpagam University in 2016. He is currently working as an Assistant Professor in the Department of Computer Science and Engineering at Karpagam University. He published 31 articles in International Journals. His area of interest is Cloud and Distributed Computing.

Ms.M.Shalini received her B.Tech degree in Information Technology from Sri Shakthi Institute of Engineering and Technology Coimbatore and now pursuing M.E degree in computer science and engineering at Karpagam University.