International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

HMAC Balanced Load Sub Cluster Head Selection for Wireless Sensor Networks

Anusha P[1], Shyjith M B[2]

[1]*MTech Scholar, Department of Computer Science and Engineering, Jawaharlal College of Engineering and Technology, Kerala, India*
[2]*Assistant Professor, Department of Computer Science and Engineering, Jawaharlal College of Engineering and Technology, Kerala, India*

Abstract -*In many sectors the Wireless Sensor Network played a critical role. But there is still a work gape in WSN in the field of energy conservation and privacy issues. Since reviewing earlier approaches, a new concept was developed using HMAC Balanced Load Sub Cluster Head Selection for WSN as Malicious Detection. A load-aware cluster-head rotation approach is also proposed, which sets a dynamic CH-rotation threshold to reduce premature death of CH nodes. The attacks including flooding attack and Sybil attack were also concentrated in the network. And also, the idea of balanced load is integrated with hybrid medium access control protocol to reduce the network's energy consumption. And the sub-cluster head selection principle works to both reduce energy consumption and also to prevent the black hole network from targeting Sybil. The results like energy output, energy consumption, packet transmission ratio, packet drop and network delay are measured during the performance review.*

Key Words: **Drowsiness detection, Hybrid Medium Access Control protocol, Sub Cluster Head, Wireless Sensor Networks, Elliptic Curve Cryptography, Energy Efficiency, Private Key, Public Key.**

1. INTRODUCTION

Wireless sensor networks consist of independent sensor nodes that are installed in a working area and track various environmental and physical conditions such as motion, temperature, pressure, vibration tone, or pollutants. WSN transmits the data across several nodes and links the data to other networks such as wireless Ethernet via a gateway. The key reason for advancing the wireless sensor network was initially military applications in battlefields but now the application scope is expanding to other fields including industrial surveillance, traffic control and safety monitoring. Various constraints such as size; cost result in resources, bandwidth, memory, and sensor node computational speed constraints.

In wireless sensor networks [2], there are a large number of nodes that are hard to replenish with minimal energy consumption. If the energy consumption is too fast, the unbalanced charge will reduce the lifespan of the node and affect the performance of the network. Therefore, it is important to research how to reduce the energy consumption of sensor nodes and increase the energy utilization rate of nodes, in order to extend the lifetime of the network. Clustering is a useful technique in which lifespan, scalability, and load balancing can be influenced by the network. Energy efficiency [6] can be achieved by using strategies that minimize the overhead and balance the energy consumption of individual nodes to the maximum possible extent.

There are different types of attacks in the networks, A Sybil attack is an attack which creates multiple identities from same malicious node. Random Password Comparison (RPC) method is to prevent Sybil attack [5]. The wormhole node will advertise is a shortest path between node [3]. Flooding attack leads to the degradation in terms of result of throughput, wastage of bandwidth, exhaustion of battery power [4].

One of the main problems with WSN is to ensure security Despite the sensors being checked by their neighbor node and using encryption estimates for insurance protection, a WSN will not spill out any of its capabilities. Wireless sensor networks are regularly measured in fixed time intervals based on the number of unsuccessful and active contact attempts made by a particular node. The problem with this recursive form of trust estimation methodology is that it places more emphasis on the node 's recent state and does not consider any past attempts at failed contact. Subsequently, by using such checked positive communications, a malicious node may simply remove any bad reputation, and the later continue to attack. During an on-off attack, for example, the malicious node switches its actions from good to bad, and from bad to good, making itself undetectable during the attack. Detecting such a state is critical for preventing resource wastage.

The paper introduces an energy efficient confidence management model for securing lifesaving information through sensor nodes with optimum power / energy usage. The model demonstrates an architecture based on a cluster of 3 tiers where the first tier records the nodes' first run configuration. The second tier secures data between nodes, and the third tier ensures energy efficiency by measuring energy consumption at each level and rotates cluster head among nodes and network working with lower energy

consumption. In terms of computational overhead, energy consumption, and throughput and data drop rate, the scheme performs better than Anonymous Authentication for Wireless Body Area Networks with Provable Protection. At last, energy efficiency is the overall requirement for third-tier architecture-energy efficiency, and the algorithm continues to measure it, and a new CH is allocated when energy consumption exceeds the defined limit. New assignment to CH is dependent on the node's trust value. To become a CH the node must attain a certain degree of trust. The advantage of existing is that the overall requirement is better, and the energy efficiency is maintained. The disadvantage of existing system is low Service Quality.

2. PROPOSED METHODS

The disadvantages of our existing system are low quality of service and privacy issues. To avoid those issues, developed the latest prototype called Malicious Detection using HMAC Balanced Load Sub Cluster Head Selection for WSN after evaluating the earlier methods. We've focused attacks in the network, including Black Hole, Sybil, Wormhole, flood attack. And the principle of sub cluster head selection works both to reduce energy consumption and also to avoid the assault on the network. The difference between the usual child nodes and the head of the sub-cluster plays a large part in energy consumption. Thus, balanced load sub-cluster head selection contributes to nominal energy depletion of each node present in the network by generating transmission between the Sub cluster heads with closer nodes by balanced load. The principle of sub-cluster head selection works both to minimize energy consumption and also to avoid black hole and Sybil attack from the network.

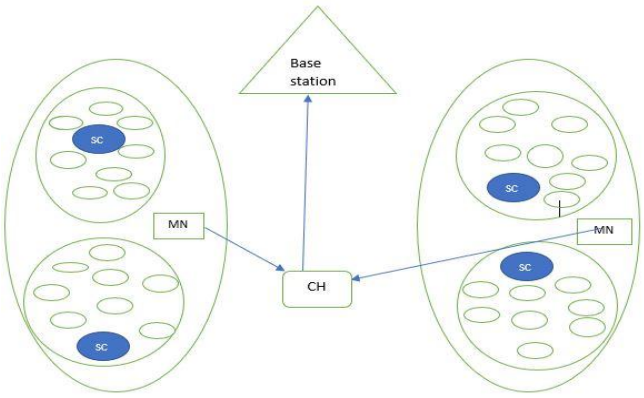


Fig 1: Architecture of proposed network

In addition to this, there is a combination of ECC algorithm and SHA-5 algorithm to provide duel authentication primarily to concentrate integrity and confidentiality. ECC is a mathematical method that can be used to construct encryption keys, stable digital signatures, and more. SHA-5 is a hashing algorithm that performs a hashing function on some data given to it. Both algorithm uses the project as dual authentication. The SCH nodes in the network send hello packets to all the nodes present in the surrounding area, and the nodes send the acknowledgment back. TDMA MAC scheduling technique for avoiding collision is introduced here. Both SCH nodes equate the distance between themselves and the child nodes with the threshold distance according to the receiving of an acknowledgement.

3. SYSTEM WORKING FLOW DIAGRAM

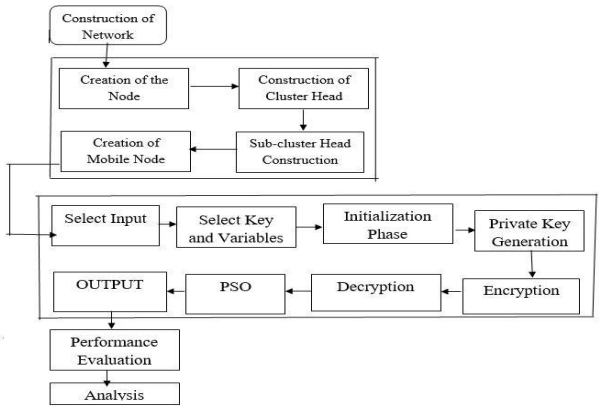


Fig.2 System work flow

The flowchart represents the project's working flow. The first flow consists of building a network. The second flow consists of creating and building nodes and cluster heads, then creates a mobile node. After creating a mobile node, the selection passes to the second flow input selection. The selection has selected key and variables, then it goes into the initialization phase and generates private key. After the private key is generated, it performs encryption and decrypts the data. Then we get the output. Evaluation of the performance and analysis at last.

4. IMPLEMENTATION

There are three main blocks in the network. First phase is the network connection. The connections between nodes are performed here. By creating the Homogeneous network, we can achieve the confidentiality in the network. We are creating a WSN here. All the device and their information remain confidential in the network or in the organization which is going to deployed this network. Second block is network stimulation. The transmissions between nodes are performed. Network is measuring the transmission power of each and every node within the network while communication in the network. Utilizing this approach even a solitary black hole and Sybil attack can be distinguished in the system. Finally, detection is the last phase. The Detection and prevention of blackhole and Sybil transmission is Performed here. In this we propose another parameter, the powerful transmission of node in Balanced load sharing. To detect the single attack from the network become very difficult task as compare to the multiple attack from the network, this can be done by this simulation. Attack

and detection and prevention from the attack by throughput, packet delivery ratio and end to end delay of the nodes.

A. HMAC Mechanism: The mechanism involved in this protocol for Hybrid Medium Access Control requires a set method after the position process and is as follows;

Initially the nodes start to identify the location 's best intermediate node. This is possible from time to time, by transmitting the word of hello. In this simulation the exchange of hello message takes place every 30sec. And the hello memory is then exchanged between nodes, allowing the nodes to find their next neighbor and the details are stored in the list of neighbors. Second, the node is starting to sense its related parameters and is transmitting the data to the destination using CSMA system. This process continues until two conditions have been met. They are (a) traffic load should not increase and (b) during the absence of transmission of emergency packets. Third, data transmission based on high priority region is initiated. If any node is identified as being in the high priority region, the neighboring nodes hold the data and transfer it to TDMA and provide the current slot to the node in the high priority region. Finally, if two nodes in the current slot occupy the high priority region, then this is assigned to transfer the information one after the other. Turn on CSMA mode at the end.

B. Balanced load SCH Selection: The balanced load SCH selection is aimed at reducing energy consumption and increasing lifetime by introducing the concept of load balancing into it. If few sub-cluster nodes are heavily loaded, this results in faster energy consumption and the balanced load sub-cluster head selection is initiated to get normal energy depletion. The distance between the normal child nodes and the head of the sub cluster plays a significant part in energy consumption. Thus, balanced load sub-cluster head selection results in nominal energy depletion of each node present in the network by creating transmission between the Sub-cluster heads (SCH) with closer nodes by balanced charge. The SCH nodes in the network send hello packets to all the nodes in the surrounding region, and the nodes send the acknowledgment back. The technique of TDMA MAC scheduling is applied here to prevent collision. Both SCH nodes equate the distance between themselves and the child nodes with the threshold distance according to the receiving of an acknowledgement. Each SCH node sends the message at the end of the distance calculation to the child nodes concerned, which are linked with it. If the child receives more than one number of copies then the SCH node to be coordinated will be selected randomly.

$DISTANCE_{(SCH)(CN)} = \sqrt{SCHa(i,j) - CNb(i,j)}$ ..... Eqn (i)

Where a= 1,2, 3, ... 10% of total the nodes

b=1,2, 3,.80% of total the nodes

SCH=Sub Cluster Head

CN=Child Node

$DISTANCE_{(SCH)(CN)} < DISTANCE_{(Threshold)}$

The balanced load principle is implemented in accordance with the network to SCH nodes, where the balanced load SCH is established in each cluster according to figure 1 of the shortest distance between the SCH nodes and the child nodes, and the distance is determined using equation 1. In the figure the SCH nodes were shown by the black filled circles and the other nodes are child nodes. The Head of the Major Cluster (MCH) and the Base Station (BS) are so far from the field where the nodes are located. Here Mobile Sink Nodes (MSN) are implemented to collect the SCH information and transfer it to the MCH node.

C. Algorithm for balanced node SCH Selection:

Step 1-SCH advertising and counter value for all SCH nodes is defined as (N / SCH)-1.

Step 2-Identification of CN nodes

Step 3-Eq.1 used with $DISTANCE_{(Threshold)}$ to calculate SCH and CN distance.

Step 4-If the counter value decreases $DISTANCE(SCH)(CN) < DISTANCE_{(Threshold)}$

In other words, counter value remains the same

Step 5-Stop comparing if CV – 0,

Step 6- When SCH exceeds CL (capacity limits), the transmission of knowledge about the rejection starts.

Step 7- Rejected CN nodes send requests to SCH node nearby.

D. Data transfer details: First, Child node transmits the information to the head of the sub cluster. Second, due to the size, the sub-cluster head node cannot pass the information directly to the head of the cluster. Mobile sink nodes are added to tackle these issues. Mobile sink mode can serve as the intermediary between the head of the sub cluster and the head of the cluster. It goes from one location to another and gathers the information from the head of the sub cluster and passes it on to the head of the cluster. Third, each sub-cluster consists of one or more mobile sink nodes based on the number of child nodes present in the head of the sub-cluster. In that case, if any of the mobile sink efficiency decreases, the sub cluster head will receive the help of the mobile sink node of the neighboring subclustered head to transfer the data to the cluster head.

E. Dual Authentication: The ECC algorithm and the SHA-5 algorithm are combined to provide duel authentication,

primarily for integrity and confidentiality. Elliptic curve method is a method of cryptography, and it is part of ECC for open key cryptography execution. The protection originates in the Elliptic Curve logarithm. The diagram is given below for the proposed ECM process.

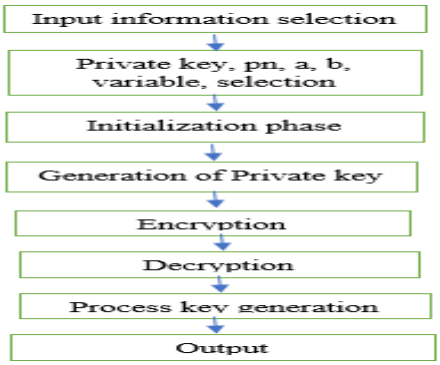


Fig.3 Proposed ECC method

F. Parameter selection process for ECM method: Curve Equation = $Y^2 \bmod q = X^3 + bX + c \bmod q$ .....(ii)

Where, (b, c) are integers and q = prime number.

G. Initialization phase: The prime number in ECM cryptography is k, and private key is P. The equation then becomes,

$E = S(i)^3 + u * S(i) + v$ ..... (iii)

Where the values u and v are unchanged, and u = v=2

The smaller key size and reduced storage are the prime benefits that ECM system offers. In general, this is only the best selected point in the elliptic curve, if the condition X = Y is satisfied. The X and Y.

$X = \bmod (E, p_n)$ ..... (iv)

$Y = \bmod ((S(j))^2, p_n)$ ..... (v)

H. Key generation: The consumer renders Ks hidden key. Since the ECM method creates two keys which are private key (PR_K) and public key (PU_K). Under gone XOR operation is the hidden key. The best point is the public key Ks(k, l) and PU_K, then the PU_K is given as,

$PU_K = PU_K * ks$ ..... (vi)

I. Encryption: Authorization-based messages or information encoding is called Encryption. Two points are given as inputs in that process. Then the data Sx(n, m) and Sy(n+lm) is,

$H_1 = PR_k * K_s$ ..... (vii)

$H_2 = (S_x, S_y) + H_1$ .....(viii)

When the transmitter key is identical and the destination key is identical then it is referred to as symmetric key generation and the transmitter key and destination key are different so it is called asymmetric key or two key generation.

J. Decryption: The reverse encryption methodology is called decryption which is the process of shifting the encrypted cipher text to the single plain text. PRk Private Key is used to decode the message.

$HD = PR_K * H_1$ ..... (ix)

The secret key PR_K is created in this decryption process by using various optimization methods such as Genetic Algorithm and PSO.

5. RESULTS AND ANALYSIS

The main concerns in a WSN system are laid in energy efficient management, optimal energy consumption, cluster head selection, drop out of packets due to attacks and life of the cluster. In this project we mainly focus to overcome these hurdles for the proper commuting of data packets. Over crowding of packets in cluster head may reduce the life span of the head node which lead the decaying of cluster much faster in-order to face these critical situation rotation of cluster head among the nodes is work implied in the proposed system.

Method	Average remaining energy	Packet delivery ratio	E2E delay	TCP packet received	TRE	Through put
LEACH	16000	60000	1	250	150	60000
E-LEACH	24000	75000	.87	350	240	54000
M-LEACH	25000	79000	.85	400	250	49000
AAWBAN	28000	85000	.65	650	300	48000
CEETM	30000	92000	.55	850	360	32000

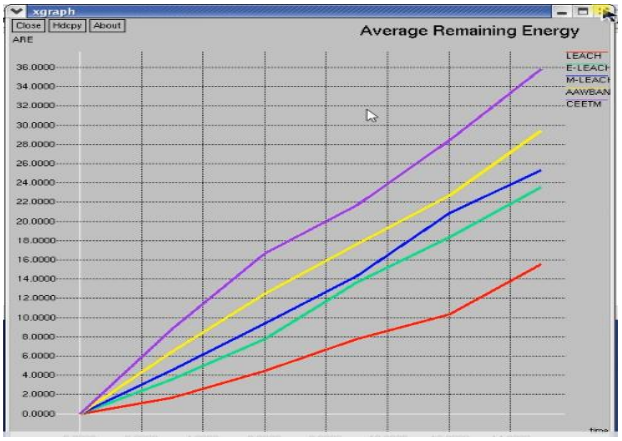
Table.1 comparison of proposed method with different methods

The three-tier model of our system improves the performance of our system parameters such as energy efficiency, throughput, reduced drop rate. Here table displays comparison of the proposed method with different methods like LEACH, E-LEACH, M-LEACH, AAWBAN.

Here calculates performance when attack or flooding occurs during transmission.

Cases	Energy efficiency	Packet drop	Packet delivery ratio
Flooding case1	54000	21000	94000
Flooding case2	27000	19000	94000
Sybil case1	30000	16000	93000
Sybil case 2	25000	15000	93000

Table. 2 Attacks during transmission



F ig.4 Average Remaining Energy

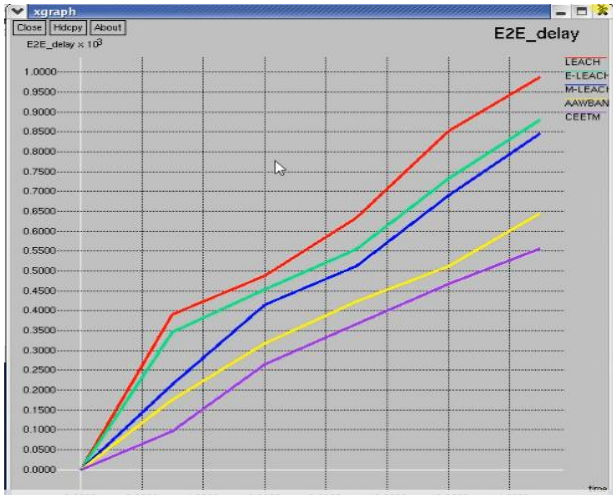


Fig.5 E2E_delay

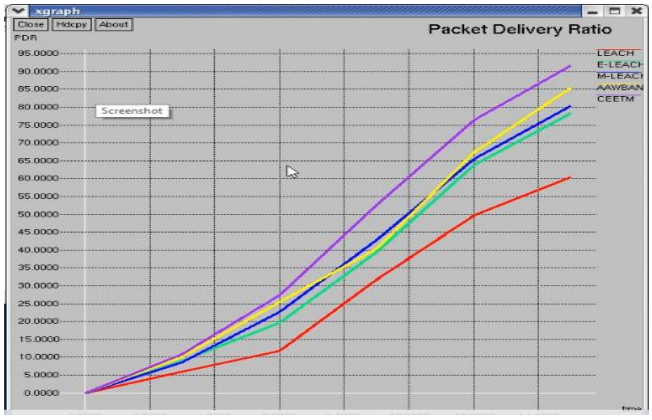


Fig.6 Packet Delivery Ratio

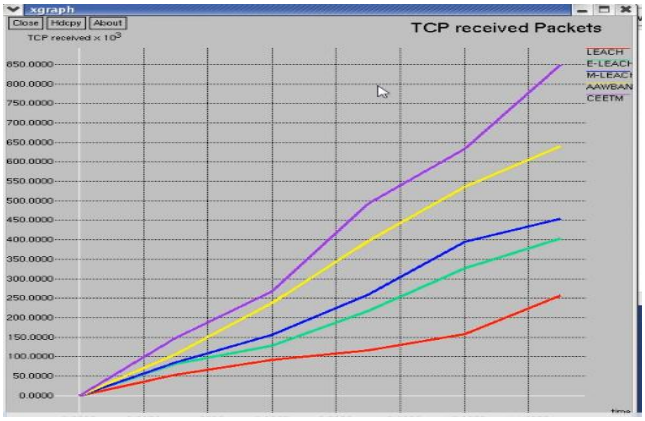


Fig.7 TCP Received Packets

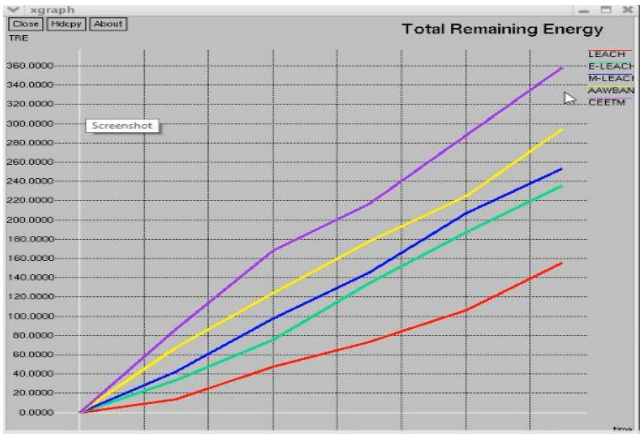


Fig.8 Total Remaining Energy

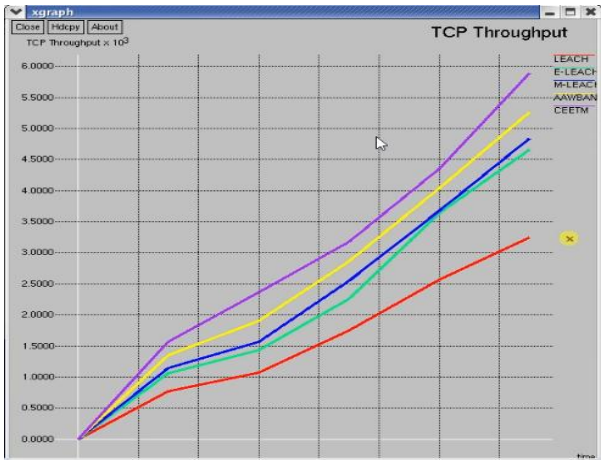


Fig.9 TCP Throughput

6. CONCLUSION

In our approach identification and moreover prevention of black hole and Sybil attack occurs by using the efficient mode of transmission. In case there is in the network a single attack that can also be distinguished and forestalled by this method. In this exploration paper we dissect the normal HMAC steering convention with attack assault and have

proposed a solution to its position problem using changed system. In modified force of transmission of each node measure by new field. For the counteractive action or security perspective we will document classification and validness to the honest to legitimate node of the system. The balanced selection of load sub-cluster head reduces energy consumption and increases lifetime by introducing the concept of load balancing into it. When few sub-cluster nodes are heavily powered, this results in faster energy consumption and the balanced load sub-cluster head selection is initiated to get regular energy depletion.

REFERENCES

1. Rohit Pachlor And Deepti Shrimankar (2018), LAR-CH: A Cluster-Head Rotation Approach for Sensor networks IEEE Sensor Journal, Vol 18, 9821 – 9828.

2. Yong-wen Du,Zhang-minWang,Gang Cai and Jun-hui Gong (2018),Load –balanced routing algorithm based on cluster heads optimization for wireless sensor networks EITCE.

3. Rajendra Kumar Dwivedi, Prachi Sharma, Rakesh Kumar (2018), Detection and Prevention Analysis of Wormhole Attack in Wireless Sensor Network IEEE,978-1-5386-1719-9

4. AKOURMIS Sana 1, FAKHRI Youssef 1, 2, RAHMANI MOULAY DRISS (2018), Flooding Attack On Aodv In Wsn IEEE,

5. Shehnaz T. Patel, Nital H. Mistry,(2017),A Review: Sybil Attack Detection Techniques in WSN, International Conference on Electronics and Communication Systems (ICECS), 978-1-5090-3355-3.

6. Shrijana Pradhan and Kalpana Sharma (2016), Cluster Head Rotation in Wireless Sensor Network: A Simplified Approach International Journal of Sensor and Its Applications for Control Systems Vol 4, 228.