Highly Secured WSN Life Span Fortification with Data Compression, NNF Technique and ECC Method

M. Nagarajan
Department of CSE
Valliammai Engineering College
Chennai, India
nagraaj_cs@yahoo.com

T. Dhanapalan
Department of Placement,
Valliammai Engineering College
Chennai, India
tdhanapalan@gmail.com

S. Jayanthi
Department of CSE
SMK FOMRA Institute of Technology
Chennai, India
jaya_dhanush@yahoo.co.in

Abstract— In WSN the major drawback is conservation of the energy available at each sensor node. Our proposed scheme consists of centralized Low Adaptive Cluster Algorithm (LEACH-C) which is a widespread protocol in Wireless senor networks to reduce the energy conception. Data compression is to reduce the number data element in a transmission. Nearest neighbor algorithm which is also used to overcome the Network traffic issues that occur due to some network collision so that the data will be lost and elliptical curve cryptography is implemented for provide security to the data.

Keywords- Data Compression, LEACH-C, NNF, Elliptical Curve Cryptography Introduction (Heading 1)

I. INTRODUCTION

In WSN is Energy Hierarchical Communication, Load Balancing, Network Coverage Wireless sensor networks nodes are connected with a base station. It is spatially distributed autonomous sensor to cooperatively monitor physical or environmental condition, such as temperature, sound, vibration, pressure, motion or pollutants. The main objectives of wireless sensor are event detection and transmission of data to the destination node. The major challenges of wireless sensor networks are Transmission of data without data loss, Efficient routing techniques, Limited Communication bandwidth. In a wireless sensor network all the nodes are work under the principles of battery power. Generally we cannot the produce the energy instead of this we can maximize the usage of energy. So each and every operation brings the node close to death. Our contribution in this paper is life time Life Time plays crucial roles in WSN.

Some old techniques which are used for enhance the energy conception in wireless sensor networks are. 1. Sleep as much as possible: whenever the nodes don't have any data transmission we can put those nodes in off state. 2. Acquire data only if indispensable: The data to be transmitted if necessary. 3. Use data fusion and compression: In order to transmit the raw data we can go with some fusion techniques it reduce the number of data elements as well as help the energy conception as well. 4. Transmit and receive only if necessary: the data to be transmitted and received if indispensable condition only because the data received is just as costly as sending. The data receiving process consumes more energy.

Some Recent Techniques to address the maximization wireless sensor networks are 1. Simplest direct communication (DIRECT) routing protocol: Each sensor node directly communicates with the base station. Since the distance is large, it consumes the energy quickly in most cases. 2. Minimum-transmission-energy (MTE) routing protocol: Improves the energy efficiency of DIRECT by multi-hop transmission. But MTE only considers the energy of the transmitter and neglects the energy dissipation of the receivers in determining the routes, thus it is not correct. 3. LEACH: Cluster heads are self elected. Every round LEACH reorganizes that cluster.

The cluster heads are selected randomly except for the sensor nodes previously selected as heads. The cluster may or may not be divided equally. If the cluster is not divided properly, each sensor node's energy consumption would increase.

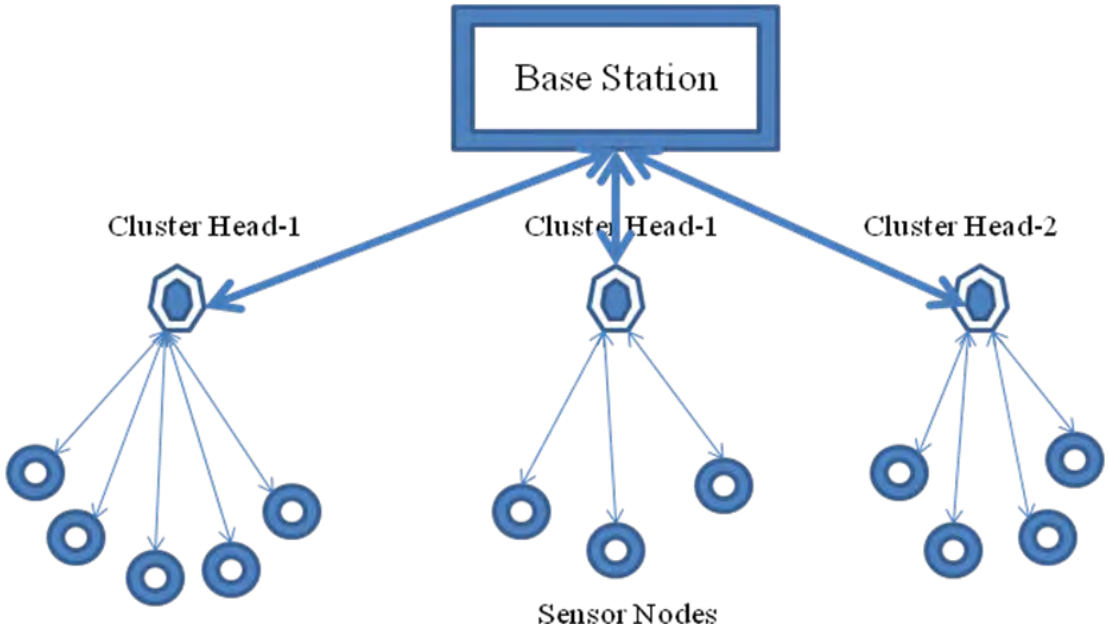

Figure I. Cluster Formation

II. PROPOSED METHOD

In the proposed method having four segment first is the data compression and second one is the Clustering third one is the nearest neighbor finding and final one is the Elliptical curve cryptography

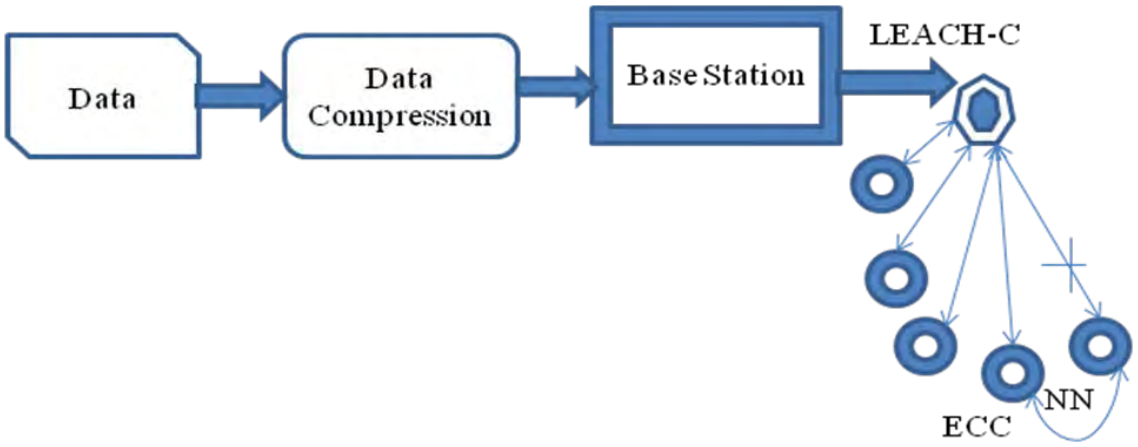

Figure II. System Architecture

A. Data fusion:

Collected sensor data packets are aggregated, combined into single packet, and redundancies in the data packets are removed to minimize data transmission. The collected data is in the form of a tuple of three values as shown in Figure II. Data item produced by a sensor node. The compression is done by checking all the most significant bits of the packets and combining the packets which have the same most significant data bits.

Source ID	***Seq. No***	***Hop Count***	***Energy Threshold***	***Signal Strength Threshold***	***Sink ID***

Figure III. Data Frame Format

A. Huffman Algorithm for Data Fusion:

Huffman coding deals with data compressions of ASCII characters. This is one of many techniques for compressing data. This method is most commonly used for emails over the internet.

B. Algorithm for Huffman coding:

1. Compute the probability of each character.
2. Sort the set of data in ASCENDING order.
3. Create a new node where the left child is the lowest in the sorted list and the right is the second lowest in the sorted list.
4. Chop-off those two elements in the sorted list as they are now part of one node and add the probabilities. The result is the probability for the new node.
5. Perform insertion sort on the list with the new node.
6. REPREAT STEPS 3, 4, 5 UNTIL you only have 1 node left.

C. Pseudo-code of the encode algorithm:

```
encode (di,Table)
IF di = 0 THEN
SET ni To 0
ELSE
SET ni To _log2(|di|)_ //compute category
ENDIF
SET si To Table[ni] //extract si from Table
IF ni = 0 THEN //build bsi
SET bsi TO si //ai is not needed
ELSE
IF di > 0 THEN //build ai
SET ai To (di)|ni
ELSE
SET ai To (di − 1)|ni
ENDIF
SET bsi To _ si, ai _ // build bsi
ENDIF
RETURN bsi
```

III. CLUSTER IMPLEMENTATION ON LEACH-C

LEACH stands for Low-Energy Adaptive Clustering Hierarchy- (centralized). LEACH-C uses centralized clustering algorithm during the initial stage, each node has to send information about its current location and energy level to the base station. The base station runs an optimization algorithm to determine the clusters for that round. Thus, LEACH-C requires the position of each node at the beginning of each round. A global positioning system GPS is required for this purpose and it is application-specific protocol architecture for wireless micro sensor networks. LEACH employs the following techniques to achieve the design goals. (a). randomized, adaptive, self-configuring cluster formation, (b). Localized control for data transfers, (c) low-energy media access control (MAC), and (d). Application-specific data processing, such as data aggregation or compression. Simulation results show that LEACH-C is able to achieve the desired properties of sensor networks. This CLEACH-C Method Considered to be a dynamic method for Data Transfer to the sink node. LEACH-C has two phases for transmit the Data. The reason we need network protocol such as LEACH-C is due to the fact that a node in the network is no longer useful when its battery dies This protocol allows us to space out the lifespan of the nodes, allowing it to do only the minimum work it needs to transmit data

A. LEACH Communication Protocol

- Randomly select sensor nodes as cluster-heads, so the high energy dissipation in communicating with the base station is spread to all sensor nodes in the sensor network.
- Set-up phase
  - each sensor node chooses a random number between 0 and 1
  - If this random number is less than the threshold T(n), the sensor node is a cluster-head.
- Cluster-based communication protocol for sensor networks,
- Adaptive, self-configuring cluster formation

- The operation of LEACH is divided into rounds
- During each round a different set of nodes are cluster-heads
- Each node n determines a random number x between 0 and 1
- If x < T(n) → node becomes cluster-head for current round

$$T(n) = \begin{cases} \dfrac{p}{1-\left(r \bmod \left(\frac{1}{p}\right)\right)} & if\ n \in G \\ 0 \end{cases} \quad (1)$$

B. Cluster Head

The LEACH Network is made up of nodes, some of which are called cluster-heads the job of the cluster-head is to collect data from their surrounding nodes and pass it on to the base station

B. Cluster-Head Selection in LEACH Algorithm

$$T(n) = 0 \quad \forall n \notin G \quad (2)$$

$$T(n) = \frac{P}{1 - P\left(r \bmod \frac{1}{P}\right)} \quad \forall n \in G \quad (3)$$

P = cluster-head probability (j/N)

r = number of the current round

G =set of nodes not been cluster-heads in the last 1/P rounds. Every node becomes cluster-head exactly once within 1/P rounds

LEACH-C is *dynamic* because the job of cluster-head rotates

C. Leach Two Phase:

The LEACH network has two phases: the set-up phase and the steady-state

The Set-Up Phase - Where cluster-heads are chosen

The Steady-State

The cluster-head is maintained

When data is transmitted between nodes

D. Set-up phase

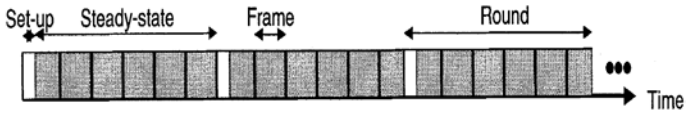

Figure.3. Time line of operation in LEACH-C

- The cluster-heads advertise to all sensor nodes in the network
- The sensor nodes inform the appropriate cluster-heads that they will be a member of the cluster. (based on signal strength)
- Afterwards, the cluster-heads assign the time on which the sensor nodes can send data to the cluster-heads based on a TDMA approach.
- Every node chooses a random number (R) and compute a threshold T(n).
- T(n) = P/(1-P*(r mod(1/p))
- if n element of G = 0 else
- P – desired percentage of cluster heads (e.g. 5%)
- r – the current round
- G – set of nodes that have not been cluster head in the last 1/P rounds
- It elects itself as a cluster-head if $R < T(n)$
- Every cluster-head broadcast an advertisement message, with the same transmit energy.
- Non-cluster-head node decides which cluster it joins in this round based on the received signal strength.

- Largest strength ◊ closet ◊ minimal energy needed for communication.

E. Cluster-Head Selection, Approach

$$T(n)=\frac{P}{1-P\left(r \bmod \frac{1}{P}\right)}\left[\frac{E_{n\_current}}{E_{n\_max}}+\left(r_s div \frac{1}{P}\right)\left(1-\frac{E_{n\_current}}{E_{n\_\max}}\right)\right] r_s = \quad (4)$$

Number of rounds a node has not been cluster-head (reset to 0 when a node becomes cluster-head)

- T(n) is increased when the network is stuck
- Possible deadlock of the network is solved

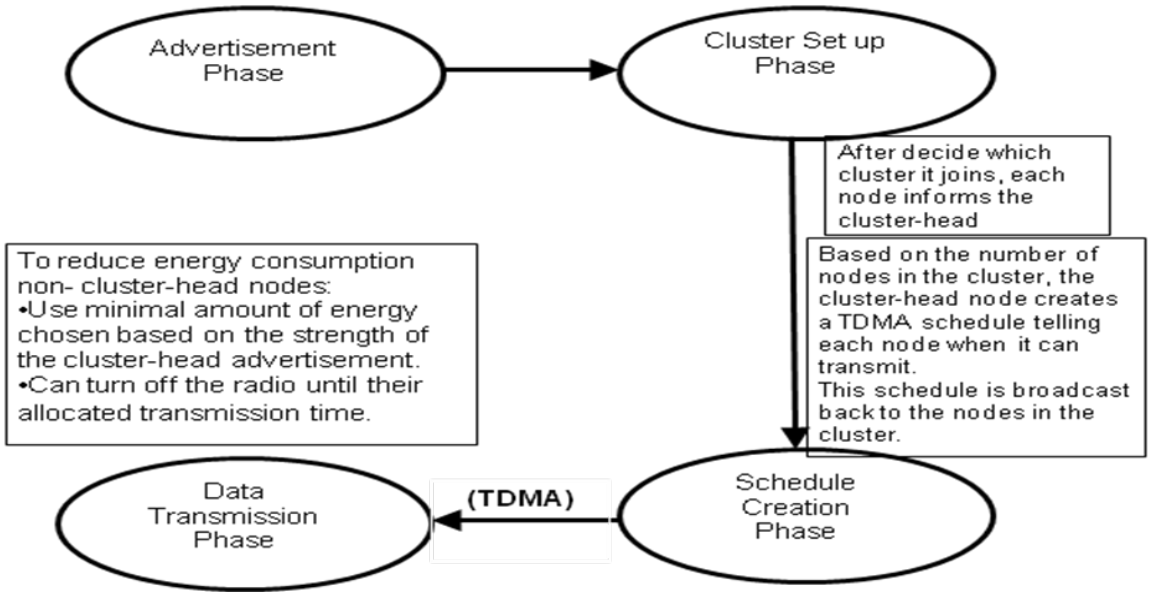

Figure IV. Operation Flow in LEACH-C

C. Calculating Lifetime:

It is used for calculating the lifetime of each of the sensor nodes. This is done in the view of recharging the nodes so as to make them efficient of handling the packets.

It is done by

$-N_{lifetime} = (1-y).B-1+(y)_{delay}$

-Where y->propagation delay

-B->Bandwidth of packets

$-y_{delay}$->delay in packet transmission

IV. SPREADING TECHNIQUES

A. Multi-hop Delay Tolerant:

In WSN data is transmitted from the source to designation, if any network traffic or network collation occurs the data packets will be lost, Once again the sender has to send the data, again there is an energy lose. To address this issue we proposed scheme called Spreading Techniques. As important challenging issues, the ensuring of each link's quality on the end to-end pathways, and enabling the data conveyance on WSN where the end-to-end route does not always exist can be listed. We developed the module that prevents weak links to be chosen as a route. This module decreases unexpected packet losses. also, we introduced multi-hop delay tolerant transfer" that chooses the best intermediate node as the next data carrier.

B. Nearest Neighbor Search:

Algorithm Multistep NN (Q,K)

1. Retrieve the k NNs(P1,…..Pk) of Q According to DST
2. RS = {P1,……..,Pk), sorted according to DST
3. DST_{max} = DST (Q1, Pk) // the current k^{th} NN DST
4. P = next NN of Q according to dst
5. 5. While DST(Q,P) <DST_{max}

6. If DST(Q,P)< DST $_{max}$
7. Insert P into RS and remove previous kth NN
8. Update DST $_{max}$ over RS
9. P=next NN of Q according to dst

C. Elliptical Curve Cryptography

The ECC is the public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications.

E -> Elliptic Curve

P -> Point on the curve

n -> Maximum limit (This should be a prime number)

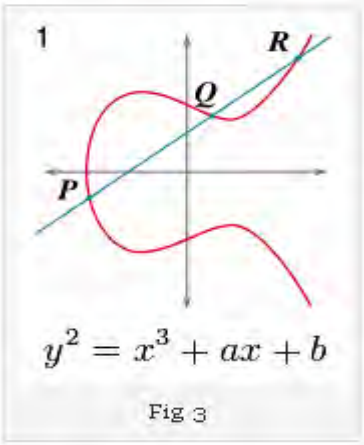

Figure V. ECC

1) *Key Generation*

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Now, we have to select a number'd' within the range of 'n'**.**

Using the following equation we can generate the public key

2) Q = d * P (5)

d = The random number that we have selected within the range of (1 to n-1). **P** is the point on the curve.

'Q' is the public key and 'd' is the private key.

3) *Encryption*

Let 'm' be the message that we are sending. We have to represent this message on the curve. This has in-depth implementation details. All the advance research on ECC is done by a company called certicom.

Consider *'m'* has the point *'M'* on the curve *'E'*. Randomly select 'k' from [1 - (n-1)].

Two cipher texts will be generated let it be C1 and C2**.**

4) C1 = k*P (6)

5) C2 = M + k*Q (7)

C1 and C2 will be send.

6) Decryption

We have to get back the message 'm' that was send to us,

7) M = C2 – d * C1 (8)

M is the original message that we have send.

8) Proof

How does we get back the message,

$M = C2 – d * C1$ (9)

'M' can be represented as 'C2 – d * C1′ (10)

$C2 – d * C1 = (M + k * Q) – d * (k * P)$ (C2 = M + k * Q and C1 = k * P) (11)

$= M + k * d * P – d * k * P$ (canceling out k * d * P) (12)

= M (Original Message)

The Elliptical curve cryptography provide the security when the data in nearest neighbor for a longer period the data might the hacked by some other person to address the issue the Elliptical curve cryptography provide the security for the data.

VI. Conclusion

In this paper we have proposed techniques for energy fortification to the sensor nodes for efficient transmission with elliptical cryptography. The main problem with wireless sensor networks is energy. We cannot produce to energy to address this issue we can increase lifetime of these networks and to reduce energy use for nodes. In this paper we have we have introduced the concepts of Data compression which reduce the number of data elements. Clustering and Spreading Techniques which enhance the transmit the data efficiently with the less energy conception.

ACKNOWLEDGMENT

I am really indebt to Our Principal Dr. B. Chidambara Rajan, Vice Principal Dr. M. Murugan, Head of the Department Dr. B. Vanathi, and our Pioneer Mr. M.Senthil Kumar Assistant Professor/CSE, for their continuous encouragement. Finally I must say thanks to Mr. R. Sankaranarayanan for providing technical support.

VII. REFERENCE

[1] M. Nagarajan, T. Geetha, "Wireless Sensor Network's Life Time Enhancement With Aid of Data Fusion, LEACH-C and Spreading Techniques", International Journal of Information Technology and Engineering, Vol.3 No.1-2 2012.

[2] Zahra Rezaei, Shima Mobininejad, "Energy Saving in Wireless Sensor Networks", International Journal of Computer Science & Engineering Survey, Vol.3, No.1, February 2012.

[3] Meena Malik, Dr. Yudhvir Singh, Anshu Arora, "Analysis of LEACH Protocol in Wireless Sensor Networks, International Journal of Advanced Research in Computer Science and Software Engineering", Volume 3, Issue 2, February 2013

[4] Li Li, Jian Li, "Research of Compressed Sensing Theory in WSN Data Fusion, Computational Intelligence and Design" Fourth International Symposium, PP 125 – 128, 2011.

[5] Capo-Chichi, M.E.P, Friedt, J.-M. Guyennet. H, "Using Data Compression for Delay Constrained Applications in Wireless Sensor Networks Sensor Technologies and Applications", Journal of Sensor Communication, PP 101 – 107, 2010.

[6] Busan , "An Energy Balancing LEACH Algorithm for Wireless Sensor Networks" Journal of Information Technology: New Generations, PP 822 – 827, 2011.

[7] Haosong Gou, Younghwan Yoo, Hongqing Zeng, "A Partition-Based LEACH Algorithm for WirelessSensor Networks" Computer and Information Technology Ninth IEEE International Conference on, PP 40 - 45, 2009.

[8] Haodong Wang, Bo Sheng and Qun , "Elliptic curve cryptography-based access control in sensor networks", Int. J. Security and Networks, Vol. 1, Nos. 3/4, 2006.

[9] R. Rathna, A. Sivasubramanian, "Improving Energy Efficiency In Wireless Sensor Networks Through Scheduling And Routing", International Journal Of Advanced Smart Sensor Network Systems, Vol 2,No.1, January 2012.

[10] Yingwei Yao, Georgios B. Giannakis, "Energy-Efficient Scheduling for Wireless Sensor Networks, IEEE Transactions on Communications, Vol.. 53, NO. 8, 2005.

[11] Satvir Singh, Meenaxi, "A Survey on Energy Efficient Routing in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, 184Volume 3, Issue 7, July2013.