ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

EE- LEACH Protocol for Secure Data Aggregation in Wireless Sensor Network

Shruthi. S, Sheethal Raj T.G

M. Tech, Department of CSE, Sapthagiri College of Engineering, Bangalore, India

Assistant Professor, Department of CSE, Sapthagiri College of Engineering, Bangalore, India

ABSTRACT: A wireless sensor network (WSN) contains a massive quantity of sensor nodes which are inadequate in vigor, storage and processing vigor. One of the important duties of the sensor nodes is the gathering of knowledge and forwarding the gathered knowledge to the base station (BS). For that reason, the network lifetime turns into the predominant criteria for mighty design of the data gathering schemes in WSN. On this paper, an energy-effective LEACH (EE-LEACH) Protocol for data gathering is presented. It offers an energy-effective routing in WSN situated on the potent information ensemble and most excellent clustering. In this procedure, a cluster head is elected for each cluster to reduce the energy dissipation of the sensor nodes and to optimize the useful resource utilization. The energy-efficient routing can be bought by nodes which have the highest residual power. As a consequence, the best residual power nodes are chosen to forward the information to BS. It helps to furnish higher packet supply ratio with lesser energy utilization. The experimental outcome indicates that the proposed EE-LEACH yields higher efficiency than the present energy-balanced routing protocol (EBRP) It is surely proves that the proposed EE-LEACH can support the network lifetime.

KEYWORDS: Wireless Sensor Network (WSN), Base Station(BS),Energy-Efficient, EE-LEACH.

I. INTRODUCTION

A wireless sensor community (WSN) includes a large quantity of small-sensor nodes used to observe areas, collect and record information to the bottom station (BS). Due to the accomplishment in low-energy digital circuit and wireless transmission, many of the applications of WSN are carried out and utilized in navy functions, object monitoring, habitat monitoring. A common WSN is composed of a huge number of sensor nodes, which can be randomly disseminated over the network. The alerts are picked by using all forms of sensors and the information obtaining unit, processing and transmitting them into a node known as sink node. The sink node requests for the sensor expertise via forwarding a query for the period of the network. When the node discovers the data matching the query, the response message is routed again to the sink node. The vigor conservation of the network may also be minimized by using enabling the porting of the nodes known as cluster heads. The data gathered from the nodes are aggregated and compressed by way of the cluster heads. After that, the aggregated information is forwarded to the BS, but it has some problems. The important predicament is energy consumption and it's targeting the cluster heads.

Encryption and key distribution are important primitives to build secure Wireless Sensor Networks (WSN). A large amount of different key distribution schemes were implemented, targeting different types of WSNs. These schemes face issues with respect to their requirements, implementations, and theoretic foundation. Though security is regarded as a standalone component of the architectures of many systems, in case of wireless sensor networks, it must get adequate attention. In most application domains, the sensors are used to collect a specific type of data from particular target areas, and the collected data are often considered secret and are not intended for public disclosure. Hence, efficient and secure mechanisms are needed to transmit acquired data securely to the appropriate recipients.

Data gathering is an efficient process for conserving vigor in sensor networks. The main motive of data gathering is to take away the redundant knowledge and retailer transmission energy. A data-gathering algorithm includes some aggregation methods to reduce the data site visitors. It reduces the quantity of message alternate among the nodes and BS. The efficiency of data gathering in WSN can also be characterized situated on the expense at which the sensing information can be gathered and transmitted to the BS (or sink node). In specific, the speculative measure to seize the demerits of assortment processing in WSN is the capability for many-to-one data collection. Data-gathering potential

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

reflects how efficient the sink can acquire sensing data from all sensors beneath the presence of interference. Performing the info-gathering operate over CH nonetheless causes large vigor wastage. In case of homogenous sensor networks, CH will soon die and re-clustering desires to be initiated. It reasons better power consumption.

II. RELATED WORK

Wang et.al [1], enhanced the security of the LEACH routing protocol for WSN using µTESLA and Exclusion Basis Systems (EBS). µTESLA is used for updating the security key and EBS is used for the key generation and distribution. Harjito et.al [2], developed a lightweight digital watermarking method for enhancing the security of Wireless Multimedia Sensor Networks (WMSNs). WMSNs are a class of WSNs that contains SNs with cameras, microphones and other multimedia devices. This method focuses on multimedia data authentication and privacy perseveration during compression and aggregation of multimedia data. Zhu et.al [3], proposed a secure and energy efficient data aggregation scheme for WSNs. The BS consists of a secret configuration matrix. Each SN knows a limited section of the matrix described as a secret share. The communication overhead is considerably reduced by avoiding the verification of aggregation integrity Sun et.al [4], proposed a secure in-network data aggregation with anomaly detection in WSNs. The false injected data are detected using Extended Kalman Filter (EKF) based mechanism. Each SN characterizes a normal range of neighboring SN's future transmitted aggregated values by monitoring the neighbor behavior and using EKF for prediction of their future states. EKF is used for effective local false data detection. A combined algorithm of Generalized Likelihood Ratio (GLR) and Cumulative Summation (CUSUM) are used to enhance the detection sensitivity. This local false detection method is combined with system monitoring to distinguish between emergency events and malicious events. Energy consumption is reduced by scheduling some of the SNs to sleep periodically Huang et al. (2010a) proposed a secure routing protocol using ID-based digital signature for cluster based WSNs. This method consists of a random oracle model where the security is dependent on the hardness of the Diffie-Hellman problem. This technique uses a dynamic clustering LEACH protocol to reduce the energy consumption. SNs are selected as CHs in rounds for fair energy consumption.

III. PROPOSED SYSTEM

Figure1.Shows the flowchart of our proposed system

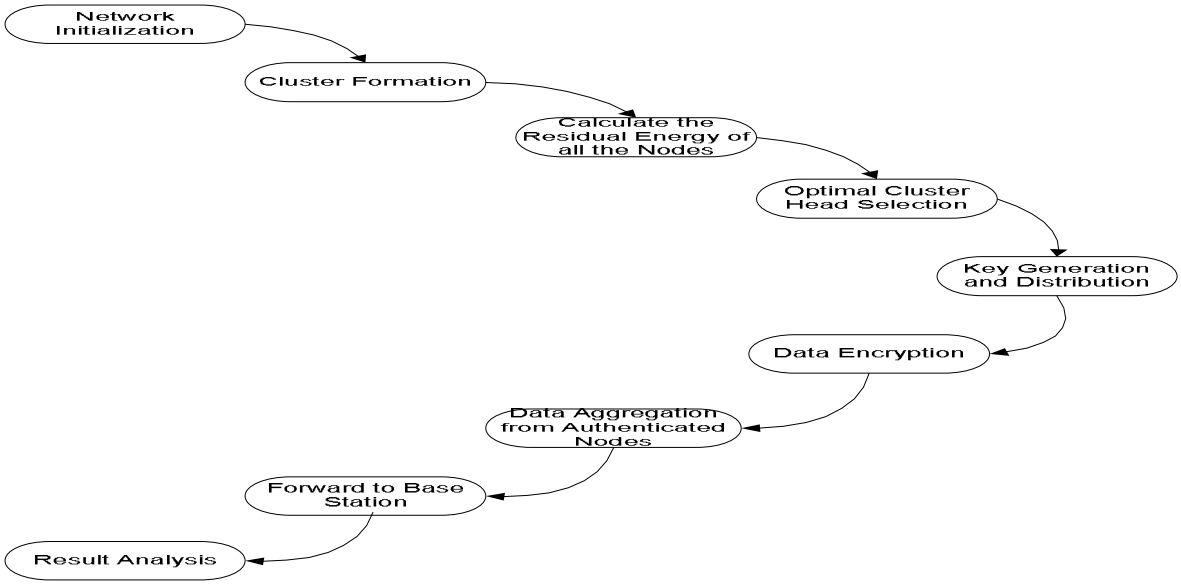

Figure 1: Flowchart of our proposed system

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

1. Cluster Formation using EE-LEACH

Energy-LEACH protocol improves the cluster head selection procedure. It makes residual energy of node as the main matrix which decides whether these nodes turn into cluster head or not in the next round.

In first round communication, every node has the same probability to turn into cluster head. $n(n = pxN)$ Nodes are randomly selected as cluster heads, and then, the residual energy of each node is different after one round communication.

We select n nodes with more residual energy as cluster heads in next round communication, and so on until all nodes are dead.

Same as the LEACH protocol, energy-LEACH protocol also divides into many rounds,
Each round contains following two phases

- cluster formation phase (Set up phase)
- cluster steady phase

In cluster formation phase,

a. Each node decides whether to turn into cluster head or not by comparing with residual energy ;
b. Some nodes with more residual energy turn into cluster heads
c. Send cluster head information to inform other nodes.
d. The other nodes with less residual energy turn into common nodes,
e. Send information about joining cluster to a cluster head ;

In cluster steady phase,

a. Nodes in a cluster send data according to TDMA table, and cluster heads receive, fuse and send data to sink.
b. After a period of time, the network reforms the cluster head selection procedure in a new round.

2. *Calculating Residual Energy*:

Before the cluster formation, the number of cluster members is unknown. However, since it is proportional to the number of neighbors near a potential CH (in a specific transmission range), the number of neighbors (defined as value$n$) could be used to obtain the expected energy consumption during the CH selection. After the cluster formation, the steady-state operation is broken into frames, where nodes send their data to the CH at most once per frame during their allocated transmission slot. In a frame, suppose a CH has n cluster members, it would receive n messages from all the members and then transmit one combined message to the base station with a distanced to BS. The number of frames could be obtained by

$$N_{frame}=\frac{t_{ssphase}}{n*t_{slot}+t_{CH\ to\ BS}} \quad (1)$$

Where $t_{ssphase}$ is the operation time of the steady-state phase, t_{slot} is the slotted time required for the transmission from members to the CH, and $t_{CH\ to\ BS}$ the time required for the transmission from CH to the base station. The expected consumed energy of a node to be a CH after a steady-state phase could be represented as:

$E_{expconsumed}(l,d_{toBS},n)=N_{frames} * (E_{Tx}(l, d_{toBS}) + n * E_{Rx}(l))$ (2)

All the sensor nodes are assumed to transmit and receive the same size of messages, i.e. l bits of data. The distance to the base station, d_{toBS}, could be computed based on the received signal strength. Then, the expected residual energy of a node to be a CH after a steady-state phase could be obtained using:

$E_{expResidual}(l, d_{toBS}, n) = E_{Residual}$-$E_{expconsumed}$ (3)

Where the $E_{Residual}$ is the residual energy of a sensor node before the cluster head selection.

3. *Optimal cluster head selection using FCM*:

The FCM's is a soft clustering algorithm; it computes the degree of belongingness in the range [0, 1].The sensor nodes compute the degree of belongingness in terms of Euclidean distance between the sensor node and the cluster head. The objective function is used to reduce the distance between the sensor nodes to the cluster head and the inter cluster distance. The FCM's aims at reducing the objective function. Euclidean distance is used to compute the distance between the sensor node and the cluster head as shown in Euclidean distance equation

Begin

a) Variables: X_i is the sensor node $i_1, \ldots$,n and y_jj is the cluster head, $j_1, \ldots$, c

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

b) Output: Calculates the Euclidean distance between each of the sensor node to different clusters.
c) For i=1 to n do
d) For j=1 to c do
e) compute the distance d(X_i, Y_jj)
f) end for
g) end for
h) End

The Fuzzy C-Means algorithm is divided into three phases:

i. Clustering calculation

The standard FCM's algorithm in our case is used to cluster the sensor nodes. The sensor nodes send HELLO packets to the base station with its GPS location, the calculation of the Euclidean distance is carried out by Algorithm 1 and then the degree of belongingness is assigned for each node by using the standard FCM's algorithm in which each node is assigned a degree of belonging to a CH rather than being a member of just one cluster. Therefore, the node with the least degree of belongingness is assigned to that particular cluster.

ii. Cluster Head selection

After the cluster is selected, other sensor nodes send data to the base station, through the cluster heads. The process of selection of clusters is repeated, only the initial decision of selection of cluster head is by the base station, and the selection of the cluster head in the further rounds is done by the existing cluster head. The sensor node with the highest residual energy is chosen as the next cluster head, the information of the residual energy is obtained from the sensor nodes during its data transmission to the cluster head.

iii. Data aggregation and transmission

After the selection of cluster head, the sensor nodes start to transmit the data to their respective cluster head. The power of transmission is optimized because of the minimum spatial distance to the cluster head is achieved. And, TDMA scheduling protocol is used, as such the sensor nodes need to turn ON their radio component during its transmission and for the rest of the time it's in OFF state. Data aggregation and fusion is done at the cluster heads, amount of data is reduced, and the CH's send the fused data to the base station.

4. Key generation and Distribution:

Generation of key using RSA:

Step1: Choose two distinct large prime numbers p and q.

Step2: Calculate the value of n.

$n = p * q$, n will be used as the modulus for both public and private keys

Step3: Find the totient of n, $fi_{(n)} fi_{(n)} = (p-1) * (q-1)$ (4).

Step4: Choose an e such that 1<e<$fi_{(n)}$ and such that e and $fi_{(n)}$ no divisors other than 1. $\gcd(e, fi_{(n)}) = 1$

Step5: Calculate the value of d based on relation,

$de \equiv 1 (mod fi_{(n)})$

Step6: keep d is private, Public key is (e,n) :public key is available to cluster members and CH. Private key is (d,n):private key is only available to the sink or base.

5. Encryption using AES

The design of AES encryption module is implemented on a chip of FPGA. Round-key generation and round operation adopt the mode of parallel computation and it can support three kinds of key length such as 128, 192 and 256 bit. The proposed scheme has the following properties: A temporary storage is used for the round operation. The processor performs each round operation while the round-key of the next round is generated. So, round-Key requires no extra storage. In this way, it not only saves the on-chip resources but also solves the delay problem caused by reading the key and it improves the clock frequency and the throughput of the system and reduced the memory requirements of the round key

After encryption all nodes checked for authentication are gathered together and forwarded to base station.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

IV. RESULTS

In this section we have computed the performance analysis for QOS parameters.

- Energy Consumption is the average energy consumed by the nodes in receiving and sending the packets.
- Packet Delivery Ratio: it is the ratio of the number of packets received successfully and the total number of packets transmitted
- End-to-end delay is the total amount of time the system takes to aggregate the data from the source to BS.

Figure2 shows the comparison graph for energy consumption between existing methods to our proposed method. Figure 3 shows the graph for packet delivery ratio verses no. of nodes.
Figure4 shows the graph for end-to-end –delay.

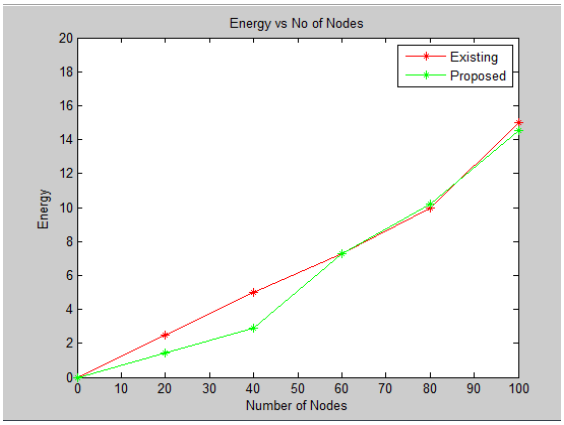

Figure2: Graph for energy vs. No.of.Nodes

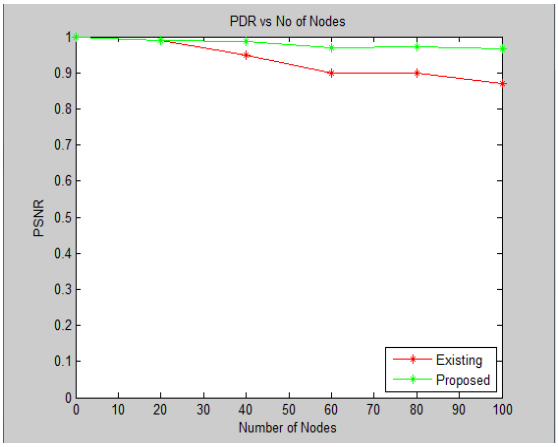

Figure3: Graph for PDR vs. No.of.Nodes

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

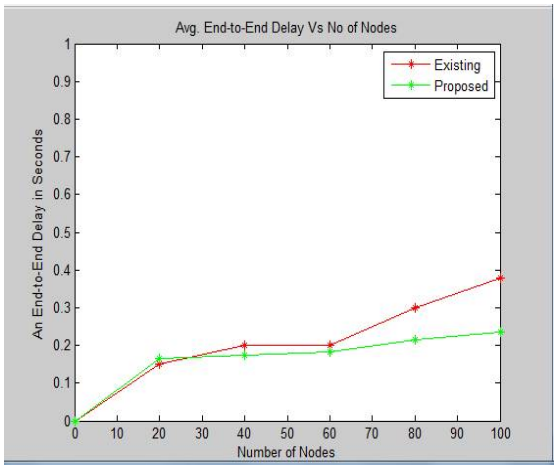

Figure4: Graph for End- to-End Delay vs. No.of.Nodes

V. CONCLUSION

In this paper shows the performance of new proposed approach EE-LEACH. We have employed Fuzzy C-Means for optimal cluster head selection by calculating residual energy of each node. Here we also used encryption schemes for providing security for data aggregation which has a significant impact on the overall reliability and energy dissipation of sensor nodes. Our method produces better energy consumption, better packet delivery ratio and better delay.

REFERENCES

[1] Wang, J., L. Zheng, L. Zhao and D. Tian, "LEACH-based security routing protocol for WSNs", Adv. Comput. Sci. Inform. Eng., Vol. 41, No. 169: pp. 253-258, 2012.
[2] Harjito, B., S. Han, V. Potdar and E. Chang, "Secure communication in wireless multimedia sensor networks using watermarking". Proceedings of the 4th IEEE International Conference on Digital Ecosystems and Technologies, pp.640-645, 2011.
[3] Zhu, L., Z. Yang, M. Wang and M, " ID list forwarding free confidentiality preserving data aggregation for wireless sensor networks. "Inter. pp. 1-14, 2013..
[4] Sun, B., X. Shan, K. Wu, Y. Xiao, "Anomaly detection based secure in-network aggregation for wireless sensor networks",IEEE Vol. 7, pp.13-25,2013..
[5] Huang, S.I., S. Shieh and J.D. Tygar, "Secure encrypted-data aggregation for wireless sensor networks. Wireless Networks", No. 16, pp. 915-927, 2013.
[6] Soufiene Ben Othman, Abdullah Ali Bahattab, Abdelbasset Trad & Habib Youssef, "Confidentiality and Integrity for Data Aggregation in WSN Using Homomorphic Encryption", Springer 2014.
[7] Josna Jose, Joyce Jose, "Asymmetric Concealed Data Aggregation Techniques in Wireless Sensor Networks: A Survey", Modern Education and Computer Science Press ,No 3, Vol 22,2014.
[8] Soufiene Ben Othman, Abdelbasset Trad, Habib Youssef, Hani Alzaid, "Secure Data Aggregation in Wireless Sensor Networks", IEEE , pp.435-785,2013.
[9] Shih-I Huang, Shiuhpyng Shieh, J. D. Tygar." Secure encrypted-data aggregation for wireless sensor networks", Springer Science 2009.
[10] Sanjeev Setia, Sankardas roy and Sushil jajodia "Secure Data Aggregation in Wireless Sensor Networks" IEEE,2012.
[11] Wenbo He, Hoang Nguyen, Xue Liu, Klara Nahrstedt, Tarek Abdelzaher. "SPDA: Secure and Privacypreserving Data Aggregation in Wireless Sensor Networks". No.1.Vol.45, 2000.
[12] T. Okamoto and S. Uchiyama. "A New Public-Key Cryptosystem as Secure as Factoring", Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques, pp. 308-318,2005.
[13] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient Aggregation of Encrypted Data in Wireless Sensor Networks", Proc. Second Ann. Int'l Conf. Mobile and Ubiquitous Systems, pp. 109-117, 2005.
[14] Homomorphism versus Watermarking Approach. ADHOCNETS 2010, 2nd Int. Conf. on Ad Hoc Networks, Dec 2009, Canada.