Kalpa Publications in Engineering
Volume 1, 2017, Pages 580–585
ICRISET2017. International Conference on Research and Innovations in Science, Engineering &Technology. Selected Papers in Engineering

Energy Efficient and Secure LEACH for Cluster-based Wireless Sensor Networks

Jignesh Joshi[1], Dr. Jagdish Rathod[2] and Dr. Kinita Wandra[3]
[1]Elect and Comm Dept of C.U. Shah University, Wadhvan, India.
[2]Electronics Engg. Dept., of B.V.M. College of Engineering, Anand, India.
[3]Elect and Comm Dept of C.U. Shah University, Wadhvan, India.
joshijh@gmail.com, jmrathod@bvmengineering.ac.in and kinitawandra.er@gmail.com

Abstract

This paper proposes energy efficient LEACH protocol for secure data transmission for wireless networks. The proposed work uses Networks Simulator – NS2.27 for the simulation of cluster based routing protocol LEACH in wireless sensor network. The work is to enhance the performance of LEACH in terms of energy saving and secure data transmission. Instead of random selection of Cluster Head (CH) the selection method is based on residual energy and vicinity of the node. With this hybrid approach, the node, which is eligible for the CH, will become cluster head and it enhances the performance of traditional LEACH. Traditional LAECH does not support secure data transmission and authentication of nodes in the clusters. By adding security between CH and CM using XOR function and key management, secure data transmission and authentication is carried out for selected application where security is the most important aspect. The proposed LEACH enhances lifetime of the wireless sensor network with security.

1 Introduction

Wireless Sensor Network consists of small tiny nodes having microcontroller based system having sensor inbuilt which senesces the parameter under application [1]. It is widely used in many applications like military for situation awareness, sensing of intruder, detection and movement of enemy on land and sea etc., in medical applications include measuring blood circulation, electro cardiogram, blood pressure, oxygen, monitoring patients health condition etc., In Energy situations applications includes fire, water, hazardous chemical level detectors, disaster management etc., and physical world applications like environmental and biological monitoring. So WSN is widely used in farming, medical and health and Industrial applications [2] [3].

A. Shukla, J.M. Patel, P.D. Solanki, K.B. Judal, R.K. Shukla, R.A. Thakkar, N.P. Gajjar, N.J. Kothari, S. Saha, S.K. Joshi, S.R. Joshi, P. Darji, S. Dambhare, B.R. Parekh, P.M. George, A.M. Trivedi, T.D. Pawar, M.B. Shah, V.J. Patel, M.S. Holia, R.P. Mehta, J.M. Rathod, B.C. Goradiya and D.K. Patel (eds.), ICRISET2017 (Kalpa Publications in Engineering, vol. 1), pp. 580–585

Wireless Sensor Networks are widely used in several important field areas because of its characteristics like size, mobility, heterogeneity, scalability to ease of use. But they have limitations and constraints of limited processing power, storage capacity radio range, bandwidth and security.

In security of WSN, there four major security aspects are confidentiality – secure data transmission, authentication – to check that who is transmitting, integrity – the data received is not tempered, and freshness – there is no relaying of the message [4]. Cryptography methods are used to maintain secure data transmission and authentication and integrity of the data [5]. The data encryption methods or can say algorithms are divided into two categories: Symmetric key algorithms and asymmetric key algorithms, which are used for secure data transmission or confidentiality. Hash functions are used for authentication and integrity. Asymmetric algorithms are consuming more energy as they require more steps to encrypt and decrypt data or data processing [4] so symmetric key approach used for security/confidentiality and hash function is for authentication and data integrity.

In this paper security or confidentiality is covered to make secure and energy efficient LEACH - a cluster based routing is discussed with its modification suggested and results to justify the proposed work. In Section II –LEACH protocol is discussed in brief, Section III –challenges in WSN, Section IV – proposed work for integration of secure data transmission and authentication with proposed methodology, Section V –results and Section VI – conclusion..

2 LEACH Protocol

The empty space on top of the first page, just before the title, will reserved for a page header containing the EasyChair logos and the volume information. This header will be added to the article when you submit it to EasyChair.

You cannot control this header placement and for this reason should not try to change vertical spacing on the first page. If by mistake you removed the empty space, you can restore it as follows. Place the cursor on the very first line of your document (that is, the first line of the title), select Format -> Paragraph in the Microsoft Word menu and set the spacing before the paragraph to 94pt and after to 15pt.

Low Energy Adaptive Clustering Hierarchy (LEACH) [1] is the first hierarchical routing protocol it is a cluster based routing protocol for wireless sensor network. LEACH operation work in the round form. In the LEACH protocol operation divided in to two phase: set up phase and steady stage phase. In the set up phase cluster organized and cluster head selection. And in the steady stage phase data transfer node to cluster head and cluster head to base station (B.S) or vice versa. Data transmission is base on the TDMA schedule.

In wireless sensor networks, Low-Energy Adaptive Clustering Hierarchy (LEACH) is one of the most effective cluster-based routing protocols.

2.1 Setup Phase:

In this phase, all node are the equally probable to develop a cluster head. Initially node become cluster head and broad cast its decision packet. In the set up phase cluster head selection priority depends on each and energy node generate the random number between 0 and 1, and then random number compare with the threshold. If the random number is less than threshold that time node are become a cluster head.

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

Where,
P = equals probability of the node in the Percentage form (0.05),
r = current round and
G = set of node that have not become a cluster head in the last 1/P round

All nodes are once again eligible to become cluster-heads. Once the cluster head has been selected that time the cluster head broadcast advertisement messages to the rest (intermediated) of the node using CSMA MAC protocol. All rest (intermediated) node receive their advertisement message from the all cluster head. After this phase each and every node decided which cluster to joint base on the signal strength. If some time may be its possible node receiving two different advertisements massages from the cluster head that time cluster head selection is based on the high signal strength. If is willing to become a member of the cluster. Cluster head receiving and transmitting information by each regular node uses a CSMA MAC protocol. In the last cluster head receives the entire massage form node that would like to joint in the cluster than cluster head broadcast the TDMA schedule in all direction.

2.2 Steady State:

After the clusters are created and the based on fixed TDMA schedule, data transmission starts. According to allocated transmission time to each regular node, it will send to data base on the TDMA schedule intermediated node sense the data and send data to cluster head than all data.

Cluster head receiver all the data receive form all intermediated node, the cluster head have received all data than the cluster-head compress all the data into a single signal. For this purpose, it performs data fusion functions. Then the composite signal is sent to the BS by the cluster-head. This is a high-energy transmission. Reason behind is the base station is far away. This steady state operation of leach network end of the steady state operation one round is complete.

3 Challenges in WSN

As discussed in Section – 2 there is a scope to enhance the WSN using one or more methods or technique for energy and security for to make WSN energy efficient and secure. The energy saving and security are the two biggest challenges in WSN.

Wireless channels are open for all so all can monitor the what is transmitted from where and most protocols used doesn't not consider security during the transmission. Security is indeed a requirement for secure data transmission and authentication of the nodes in the cluster [4].

In wireless sensor network because open channel the data transmission should be secure and the nodes in the clusters must be authenticated before data receive from the nodes as well as the data received must have ingrate fulfilled that it is not tempered data.

4 Proposed Work For Integration of Security

NS2 is used by researcher to simulate routing protocol for different kind of network configurations. For proposed work to make LAECH energy efficient and for secure data transition between CH and CM sensor nodes over WSN. Then CH election is performed and forming cluster using hybrid (residual energy and vicinity of the node) approach LEACH protocol. When CM transmits data to its CH it uses XOR data packets with pad and CH will use same pad and XOR the received packet again to get the original data packets. This paper simulated XOR function for security with key distribution for authentication of the nodes in the cluster.

The proposed work, Energy Efficient and Secure LEACH. No change in startup phase (cluster formation phase). For Security, Authentication and Integrity.

Parameters	Description
NS-2 Version	2.27
Channel Type	Wireless Channel
Antenna	Omni Directional
Cluster-based Routing Protocol	LEACH, MOD-LEACH (Energy Efficient), XR-LEACH(Secure)
Total No of Nodes	100
Initial Energy	2 joule
Area	100
One Node (BS)	Infinite Energy
BS location	(50, 175)

Table 1: Simulation Parameters/Scenario

4.1 After startup Phase (cluster formation completes)

CH generates N1, N2, … Nm (16 bit number) for each nodes in the cluster as a secret key, where m = no of non-cluster nodes in respective cluster

#N1, N2 shared between CH - N1 || CH || N2 # 1st round, for each round the above 16 bit key distribution will be done

4.2 Before data transmission

Nodes N1, N2… Nm → MAC msg (Message Authentication Code)
msg ^ N1, msg ^ N2, … msg ^ Nm
MAC calculation : MAC msg = MSG + (msg0-16 ^ msg17-32 ^ ….msgX-Y)
N1 send dt_pack (data pacjets) & MAC msg CH in TDMA schedule

After receiving dt_pack @ CH
CH recalculate MAC msg using N1= R-MAC msg (Received MAC)
$ IF received MAC msg == (R-MAC msg) ???
Yes then N1 authenticated; No then N1 is not authenticated (attacker)

5 Results

We have simulated Cluster-based Routing Protocol LEACH and proposed LEACH using NS2.27 with section V simulated Scenario. The results evaluated for the performance using the following metrics Residual Energy, Number of Data Packets Sent, and Number of Alive Nodes with respect to Time. The simulation results are presented below. The simulation results for conventional LEACH and proposed LEACH are compared for the above metrics. The graphs and tables show the results of MOD-LEACH and XR-LEACH. XR-LEACH is using hybrid approach for selection of CH which is use of vicinity in cluster formation and use of residual energy and distance of the node to BS as well as for the data aggregation for secure data transmission it is using XOR function for secure data transmission.

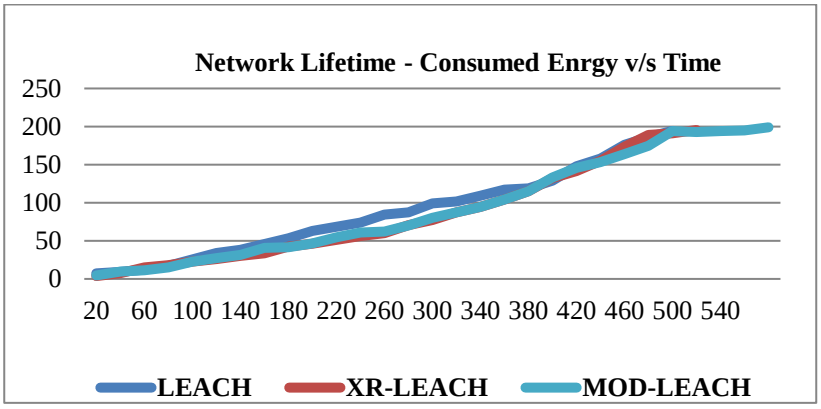

Figure 1 : Network Life Time Consumed Energy v/s Time

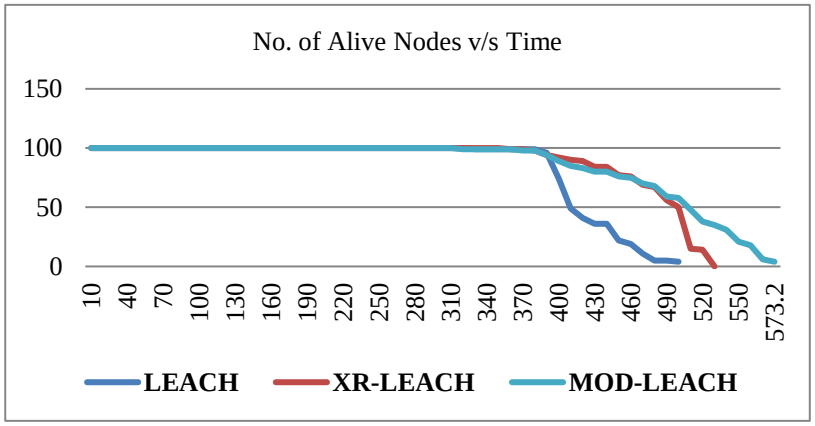

Figure 2 : No. of Alive Nodes v/s Time

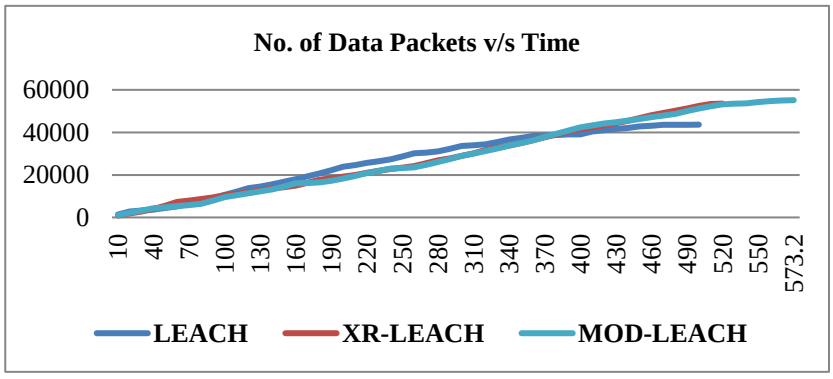

Figure 3 : No. of Data Packets v/s Time

6 Conclusion and Future Work

Secure and Energy Efficient cluster-based routing protocol (LEACH) is simulated using NS2 by changing the cluster head selection process of traditional LEACH which is random. Here in proposed work use residual energy and vicinity of the node to select CH to make it energy efficient and use of XOR function for secure data transmission from CM to CH. From the results it is concluded that the suggested XR-LEACH is Secure and Energy Efficient.

Modification in LEACH routing during establishment of cluster-head formation based on the Residual energy parameter and vicinity is added and simulation results improve in terms of energy, no. of alive- nodes, data packets – all with respect to time.

Here the results and graphs discuss in results section are for secure LEACH (XR-LEACH). The suggested algorithm in proposed work will make the LEACH secure for secure data trnasmission, authentication and with data integrity.

7 Acknowledgment

Research is a collaborative activity, in my research work there are few people to whom I recall at this point of time who directly support me to carry out my research activity. Here I would like to take a note of those people. Firstly from bottom of my heart I am highly thankful to my guide, Respected Dr. Jagdish M. Rathod, Associate Professor, Electronics Engineering Department, B.V.M. Engineering College, Anand, V.V. Nagar for his expertise teaching and guidance to assist me and my work to shape for the academic fulfillment. I am very much thankful of my internal guide Dr. Kinita Wandra, C.U. Shah University Last but not the least I am very much thankful to Mr. Mohit Tahiliani, Assistant Professor, NITK, Suratkal who his expert in Network Simulation tools and his expert session with hands on make me good to carry out my research work in simulator tools.

References

W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan (2000), *"Energy Efficient Communication Protocol for Wireless Micro sensor Networks", in Proc. 33rd Hawaii Intl. Conf. on System Sciences (HICSS'00)*.

T. V. U. Kiran Kumar and B. Karthik (May 2013), *"Improving Network Life Time using Static Cluster Routing for Wireless Sensor Networks, Indian Journal of Science and Technology, Print ISSN: 0974-6846.*

W. Heinzelman, A. Chandrakasan and H. Balakrishnan (October 2002), *"An Application-Specific Protocol Architecture for Wireless Microsensor Networks", IEEE Trans. Wireless Communications,*

Xueying Zhang,Howard M Heys, and Cheng Li (2010) *"Energy Efficiency of Symmetric key Cryptographic Algorithms in Wireless SensorNetworks", 25th Biennial Symposium on Communications IEEE, pp168-172.*

Ruiping Ma, Liudong xing, Howard E.Michel,Vinod M. Vokkarane (2012), *"Linear Cryptanalysis of A Survivable Data Transmission Mechanismfor Sensor Networks",pp-562-567,IEEE.*