ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2019.0294

HETEROGENEOUS LEACH PROTOCOL WITH SINK NODE PROTECTION IN A WIRELESS SENSOR NETWORK

Bhagyshree Pawde and Bharathi Shetty

Department of Information Technology and Engineering, Walchand College of Engineering, India

Abstract

Wireless Sensor Network (WSN) is the group of sensing computing and communication components that gives ability to sense a physical phenomenon in a specified environment. The main problem of WSN is energy consumption or battery power, to avoid such problems different type of routing protocols is used. LEACH routing protocol is used to reduce the energy consumption and enhance the battery power and network lifetime. Homogeneous LEACH has some limitation and there is no security provides to sink node. To overcome this limitation of Homo LEACH protocol heterogeneous LEACH protocol with sink node security is used in this paper. In a heterogeneous LEACH two or more different types of nodes with different battery power and functionality are used. Sink node is a sensor node which has large energy capacity and it collects data from other node. Sometime sink node affected by different type of attack such as sinkhole, black hole attack etc. to avoid these types of attack various technique are used such as intrusion detection, watchdog scenario etc.

Keywords:

LEACH Protocol, Clustering, Heterogeneous WSN, Energy Consumption, Network Lifetime, Cluster Head, Base Station

1. INTRODUCTION

WSN is the collection of small sensor node also called as a mote. Nodes sense the physical phenomena from environment. The battery is an essential part of the sensor. LEACH is standard homogeneous protocol and also it has some version with particular modification. Such as A-LEACH, C-LEACH, M-LEACH, T-LEACH etc.

The sensor having same functionality i.e. battery power, sensing range, bandwidth and also physical characteristic deployed over a region by using clustering topology to form a network and that type of network is called as the homogeneous network. LEACH is standard homogeneous protocol and also it has some version with particular modification such as A-LEACH, B-LEACH, C-LEACH, T-LEACH, and MOD-LEACH.

The steady-state phase consists of the transmission of data according to TDMA scheduling from the sensor node to CH within the cluster and then CH sends this information to the base station. BS can convert the information into the human-readable form. LEACH protocol has advantages of clustering to reduce energy consumption and enhance the network lifespan. Whereas network lifespan is a time interval or time span from starting of a network to first node death.

Network scalability means to increase or reduce the no. of the sensor node in a particular cluster network according to its work or load. The load is a collection of data on that particular node itself. TDMA scheduling reduce the energy consumption because in TDMA scheduling some time span is allocated to sensor node so that each and every sensor send the data to the CH of that particular cluster within allocated time slot hence data redundancy will be reduced and efficiency will be increased.

Every coin has two sides so that LEACH has some drawback such as all sensor nodes have same functionality, parameter, and characteristics so that while working if one of the sensor nodes is destroyed or crashed then the whole network is affected. While choosing the CH according to probability if low energy sensor node is chosen then the network lifespan and performance of a particular task will be reduced. Sometimes the distance factor between the sensor nodes in the network will be affected by the performance of the whole sensor network.

Table.1. Difference between homogeneous and heterogeneous LEACH

Homogeneous Network	Heterogeneous Network
WSNs having nodes of same energy level and almost same parameter such as range, battery power, also all sensor node are identical then such type of network is called as a homogenous WSNs	In heterogeneous WSNs, nodes are deployed with different initial energy levels, range, battery power than such type of network is called as a heterogeneous network
It saves energy but does not help in prolonging network lifetime	As compared to homogeneous it saves more energy and helps in prolonging the network lifetime
They are less suitable for real-life applications because it has some limitation due to homogeneity.	They are more suitable for real-life applications cause its Maintain heterogeneity.
Examples: LEACH, PEGASIS	Examples: DEEC, EDDIEC

The work defined in the literature of LEACH Protocol on Homogeneous network which is having sensor nodes with the same parameter which doesn't work efficiently and it has some limitation over a distributed area.

Existing approaches in this area reside big-challenges like the situation where the Sink node affected by a different type of attacks. Due to these limitations, existing approaches are not suitable for sink node security also.

In construct, take a LEACH Protocol on Heterogeneous Wireless Sensor Network with sink node protection.

In this paper, section 2 is focusing on literature related to the proposed work. In section 3, the proposed work for heterogeneous LEACH is discussed. Section 4 shows the results using LEACH protocol. Finally, in section 5 conclusion is mentioned along with the references used.

2. LITERATURE SURVEY

In [2], the author(s) said that deterministic CH selection approach to enhance the lifetime of the network and consume the remaining energy level of the particular sensor node and for that it used the threshold value formula $t(n)$, whereas it minimizes the threshold value of a particular cluster formation process.so the sensor node distance does not affect a network. By extending the stochastic CH selection of LEACH protocol with the deterministic component to reduce energy consumption.

In [3], the author(s) described the selection of cluster based on different topology because according to topology changes the whole throughput of the particular sensor network is change i.e. depends upon topology the performance of the network depends. They compare that different version of LEACH on homogeneous sensor network so that it optimizes performance by using parameter such as mobility, scalability, self-organization, distributed organization, centralized, etc.

In [17], the author(s) described that LEACH protocol and the possible attack on routing protocol. LEACH protocol having no of rounds to select the CH of the particular cluster after the formation of it so at that time the no. rounds are divided into two phases one Scheme and hierarchical routing protocol and it uses clustering topology. After deployment of the sensor node according to its parameter then formation a network called a cluster. All is a set-up phase and another is a steady state phase and no. of step in each phase. So that energy consumption will be reduced and growing the network lifespan.

In [20], the author(s) described that maximize the lifetime of the network by using clustering topology. Clustering is an important topology factor in the wireless sensor network. Also, they said about energy efficient heterogeneous network by using the sensor node having different functionality. Also, route identification technique so that it has minimum time requires sending the packet from source to destination so energy consumption is reduced and enhance the network lifespan.

In [19], the author(s) described the total information about the sinkhole attack. That is a sinkhole attack is which type attack how it works on LEACH protocol how its affected on sink node and how to apply by using mint route protocol, challenges in detection of sinkhole attacks such as communication pattern, predictableness or some existing approach such as rule-based, anomaly detection, statistical method anomaly detection method etc.

In [18], the author(s) described security requirement such as data confidentiality, data integrity, data authentication, data availability, source localization, self-organization, data freshness etc. to avoid attacks and challenges on the sensor network. Also, they describe the classification of security thread which is based on routing, capability and protocol layer and types of attack of the sensor network to avoid such type of attack some protocol is used such as SPIN, TINYSEC, LEAP, ZIGBEE etc. also they compare the all security protocol performance with all security requirements to verify the effective outcome.

In [12], the author(s) described various threat affection on various layer such as for physical layer the jamming and tampering for data link layer collision, exhaustion, unfairness for network layer sinkhole black hole, selective forwarding, for transport layer flooding, false messages for application layer data aggregate on distortion etc. this type of threats attack different layer and disturb the whole scenario of arranged WSN. Also, they discussed various launching technique to launch a sinkhole attack for e.g. IDS Architecture and working or intrusion mechanism also.

3. PROPOSED WORK

LEACH protocol is self-adaptive routing protocol which adapts or observes a sudden change in environment so that LEACH protocol is very useful to check or physical phenomena in the environment. It is a topology based sensors have the same functionality and characteristic so that the formed network is called a homogeneous sensor network. LEACH is fully implemented homogeneous sensor network routing protocol. The cluster has one node called as a CH and other is normal sensor node. According to residual energy, the CH is selected. All sensor nodes can sense the environmental phenomena and store on it then forward to that data to the CH. Formation of a cluster for LEACH protocol is the only purpose to reduce energy consumption. Improve scalability and network lifespan. Every sensor node selects a random number between 0 and 1. If this random number is less than a threshold value $T(n)$ that node is chosen as a CH for that current round. An equation of calculating the threshold value

$$t(n) = \begin{cases} \dfrac{p}{1 - p * r \bmod \left(\dfrac{1}{p}\right)} & n \in G \\ 0 & otherwise \end{cases} \tag{1}$$

where,

p is the percentage of choosing CHs.

r is the current round.

G is the set of sensor nodes that have not been CHs in 1/p rounds and n - no. of the sensor node

LEACH protocol has two phases for each round one is the set-up phase and another one steady state phase consist of cluster formation. The protocol is very useful to check or use physical phenomena in the environment. It is a topology based scheme and hierarchical routing protocol and it uses clustering. Actually

3.1 SET-UP PHASE

It consists of the cluster formation on randomly deployed sensor node in the sensor network. And each cluster consists one CH depends upon how much energy it contains. In this mode changes the information such as node ID, location, energy, etc.

3.2 STEADY-STATE PHASE

It consists the data transmission among non CH node i.e. normal node and CH in the particular cluster that data transmission happened according to TDMA (Time Division Multiple Access) fashion. By using TDMA Scheduling CH allot particular time slot to each and every sensor node to the cluster to transmit their data towards CH. So that all sensors remain inactive till their time slot does not allow to it.so that the energy will less reduce and ultimately network lifespan will be more.

When these two states finish their work then network retreats into the set-up mode and begin an alternate round, starting with a choice of a new CH. Cluster is nothing but a group of a sensor node in which all sensor node is normal sensor node and having the same functionality and among that node one sensor node is CH which has more battery power. In a cluster, all sensors sense the physical phenomena in the environment and collect it and transmit to the CH accordingly.

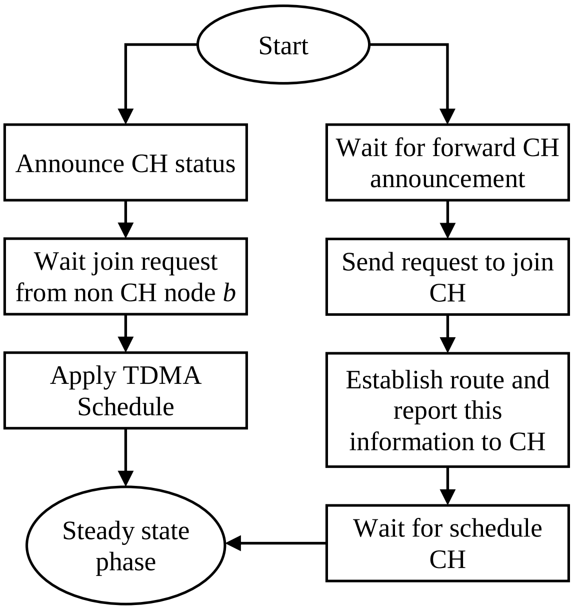

Start
Announce CH status
Wait join request from non CH node *b*
Apply TDMA Schedule
Steady state phase
Wait for forward CH announcement
Send request to join CH
Establish route and report this information to CH
Wait for schedule CH

Fig.1. CH formation

3.3 CLUSTER FORMATION

In LEACH protocol there are different methods w.r.t. attributes and algorithm to form a cluster such k-mean algorithm, fuzzy logic etc. but in LEACH protocol cluster formation in this way.

After the formation of cluster CH will select which depend upon energy constraint. Cause we reduce energy consumption and enhance overall throughput of experiment. These flow shows the activity of CH where suppose one node is CH if that node is really CH then he announces his current status i.e. I am a CH of current round and he waits to join request from another normal node then he apply TDMA (Time Division Multiple Access) and send data to the BS.

In each round selected CH broadcast an advertise message to all the nodes in the network informing their new status after receiving this message each sensor node can determine to which cluster they belong based on received signal strength according to no. of nodes in a given cluster, the cluster head generates a TDMA schedule and broadcast a transmission time slot to CH.

If the node is not CH then he waits for forwarding CH announcement from CH of that respective round, then he sends the request to join to the CH then he establishes the route and reports all information to CH then he waits for scheduling from CH. After doing this task from CH and non CH the whole scenario is going to steady-state phase.

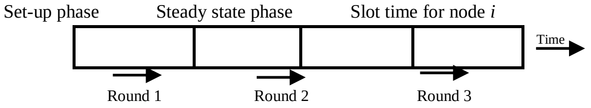


Fig.2. Time Division Multiple Access

It is a channel access method network for shared medium i.e. wireless sensor network it allows to share a same transmission medium so that all sensor node use same frequency channel and use it in their particular allotted time slot assigned by CH. With TDMA scheduling all sensor node is data sense and transmit one by one so that data should be sent to CH in a uniform manner and it avoids the same data which come from two different node and CH also reduce the redundancy of data.it prevents an intra-cluster collision.

4. ENERGY RADIO MODEL

First order radio model is used to calculate the energy consumption when bit data can transmit from sender to receiver. And this data can be transmitting from sensor node to CH and CH to BS.

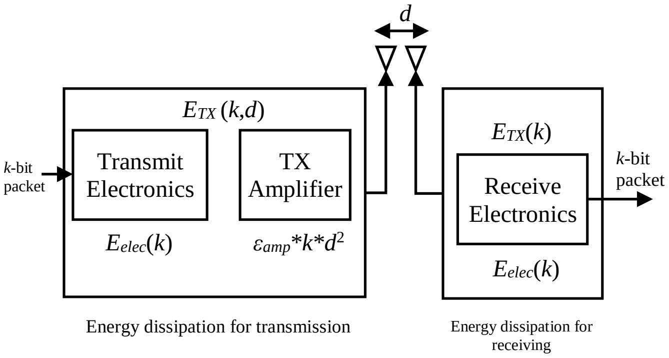


Fig.3. Energy Radio Model

The radio energy model is shown in Fig.2. Hence to transmit *k*-packet at a distance d the radio uses up is given as:

$$E_{Tx}(l,d) = \begin{cases} lE_{elec} + lE_{fs}d^2 & d < d_0 \\ lE_{elec} + lE_{mp}d^4 & d \geq d_0 \end{cases} \tag{2}$$

$$E_{Rx}(l) = lE_{elec} \tag{3}$$

where,

E_{TX} is the required energy utilization for packet transmission.

E_{elec} is electronic energy that counts on the filtering, modulation the digital coding and spreading of the signal.

$E_{fs}d^2$ (free space model) or $E_{mp}d^4$ (multi-path model), depends on the distance to the receiver and the acceptable bit-error rate.

E_{RX} required energy utilization for packet receiving and

E_{DA} is equal to the square root of the dividing EDA free space model and multipath fading model.

Both models are relying on the distance between the receiver and transmitter. Their value depends on the circuit amplifier model we use a first-order radio model. Whereas it calculates the distance in between two sensor node within a cluster and random function use for sensor distribution within a cluster.

In basic LEACH to find the distance between two hope i.e. Threshold value distance

$$d_0 = \sqrt{\frac{E_{fs}}{E_{mp}}}, E_t = 0 \tag{4}$$

$$s(i)\cdot x_d = rand(1,1) * x_m \tag{5}$$

$$s(i)\cdot y_d = rand(1,1) * y_m \tag{6}$$

where

E_{fs} is the amplification coefficient of free space signal

E_{mp} is the multipath fading signal amplification co-efficient

E_{DA} is the data aggregation

4.1 ENERGY DISSIPATION CALCULATION

Energy dissipation is degradation of energy and irrecoverable energy where energy can transform from one phase to another phase. Energy dissipation calculates on the basis of amplifier and the signal transmission, modulation, distance in between transmitter and receiver, filtration bit error rate toleration etc.

$$s(i)\cdot E = \begin{cases} s(i)\cdot E - 3000(E_{TX} + E_{DA}) + 3000E_{mp}d^4 & d > d_0 \\ s(i)\cdot E - 3000(E_{TX} + E_{DA}) + 3000E_{mp}d^2 & d \geq d_0 \end{cases} \tag{7}$$

If adding transmission energy and data aggregation energy with each other w.r.t. no. of rounds, then energy dissipated rate is calculated by transmit amplifier for the distance which is greater than threshold value (d_0) then it goes to multipath fading model (d^4) and if the distance which is less than threshold value (d_0) then it goes to free space model (d^2).

Election of associated CH for Normal Node:

$$\min(d) = \sqrt{s(i)\cdot x_d} - \left(s(n+1)\cdot x_d\right)^2 + s(i)\cdot y_d\left(s(n+1)\cdot y_d\right)^2 \tag{8}$$

CH can be elected with round by round to sending the data to BS. By using the Eq.(8) associated CH for the normal node is elected.

This all technique or formulas used in Homo LEACH protocol. In Hetero LEACH there are two types of nodes are used one is a normal node and another one is an advanced node and that is the main difference between Homo and Hetero LEACH.

Random Election of Normal Node (Hetero LEACH):

$$temp_{rand0} \geq m * n + 1 \tag{9}$$

$$E_t = E_t + s(i)\cdot E \tag{10}$$

$$s(i).\text{ENERGY} = 0 \tag{11}$$

Random Election of Advanced Node (Hetero LEACH):

$$temp_{rnd0} \geq m * n + 1 \tag{12}$$

$$S(i)\cdot E = E_0 \times (1+a) \tag{13}$$

$$E_t = E_t + s(i)\cdot E \tag{14}$$

In hetero LEACH protocol a normal and advanced node is elected by using above formulas whereas sensor node has assigned different initial energy and these sensor nodes are randomly elected with their respected energy level.

4.2 SINKHOLE ATTACK

Sinkhole attack is one type of active attack i.e. it alters or exchanges the information and change the network working. It also gives the access of network to the unauthorized person and cracks the confidential information. Sinkhole attack works on the network layer where the one sensor node act as a malicious node which has high energy level and it attracts all remaining sensor node to send their packet towards it also it sends fake routing information towards all the sensor node and also it grab the packet or information about packet through routing table of any sensor node and also it is resides in middle position in any network purposefully so it works better and fast and it creates an environment in such a way that it attacks easily and fast on the particular network.

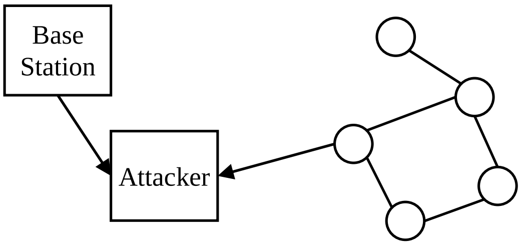


Fig.4. Sinkhole Attack

The sensor node who applies attack on the network is called as malicious node or intruder or compromised node. LEACH is routing protocol so that the attacker can easily attack with the help of routing table cause in a particular network there are no. of sensor node. In LEACH protocol firstly cluster form in a network so the in one cluster there is no. of sensor node and one is CH so all sensor node can sense the data and transmit to the CH one by one so in this scenario the communication has happened from many sensor nodes to one CH.so that the attacker can launch attack easily and make the network bulky. It can also be used to send alter and fake information to a base station. Sinkhole attack launches some other attack such as network layers replaying information, Selective forwarding or black holes, Sinkholes, Wormholes, Sybil attacks, Spoofing or Node replication attacks, Hello flood. Because of sinkhole attack change all characteristic of network such as topology, size of network, malicious node etc. And also network parameter such as data transmission and energy consumption, throughput, packet delivery ratio, etc. where data transmission is number of packet send to sensor node to base station.

Energy consumption is how much energy is consumed or absorbed by the sensor node while it's working. Throughput is overall successful packet delivery ratio; data transmission is sending packet from the sensor node to base station. For launching the sinkhole attack there are some method such as mint route protocol and TINY AODV protocol etc.it totally depend upon routing metric so the attacker can make network vulnerable by altering the routing metric.

This is the most common drawback for routing protocol i.e. the routing metric and that's why all routing protocol can easily affected by the different type of network attack. Sinkhole attack is a physical type of attack so that the attacker can easily launch an attack on a node physically and easily access all information of that particular sensor node.

4.3 LEACH WITH THE ATTACK

The formula attack can be performed on one node which is act as a malicious node whereas it collects data on itself and shows his status to all sensor nodes that is it has large battery power and drop the packet during the epoch.

$$epoch = \text{mod}(r, round(1/p) == 0) \tag{15}$$

The total number of rounds in which all nodes have become CH once.

$$\mathrm{E}_{11}(r+1) = 0; \tag{16}$$

For i = 1:100

$$E_{11}(r+1) = S_1(i) = E + E_{11}(r+1) \tag{17}$$

E_1 is the energy left for the round.

After number of round perform CH check what amount of energy is left to perform more operations.

$$E_{c1}(r+1) = E_t - E_{l1}(r+1) \tag{18}$$

E_t is the total energy,

E_c is the energy consumed till previous round

$$temp_{rand} \leq \frac{p}{1-p\,\mathrm{mod}\left(r, round\left(\frac{1}{p}\right)\right)} \tag{19}$$

This formula is used to election of CH for next round. The attack is applied during epoch in different no. of rounds.

4.4 INTRUSION DETECTION

The Intrusion detection system contains one software or device which monitors the network for illegal or malicious behavior. The device which placed in a center point within a network to monitor all the network and packet transmission in between all devices.it analyzes the whole traffic from source to destination. While analyzing the network if illegal or malicious activities are sensed or observed then some notification or alert goes to the source node.in intrusion detection some functions are used to detect the attack e.g. Path rater.

4.5 WATCHDOG

Watchdog is a timer. It starts when packet send from source to destination. Watchdog timer start Once packet send from source to the another node then that packet forwarded to the next hop node. Source node set the watchdog timer duration at time of packet sent. Source node checks the watchdog timer whether the intermediate node forward that packet to the next hope node or not within allocated watchdog timer duration. Malicious node does not send or forward any packet that it receives hence watchdog timer get expires. There is one counter present which count how many times watchdog timer get expires. Source node set the failure threshold value of watchdog timer expires. Once counter reaches that failure threshold value then that node is declared as a malicious node hence we block that node, delete route cache and stop working of that particular node. In this way by using watchdog timer we can prevent attack.

4.6 PATH RATER

To detect the malicious node and to validate the route path rater function is used. When node transmits the packet from source to destination they maintain their routing table. While transmitting the packet, nodes are updating their routing table. Path rater function checks the route reply process and route cache for the malicious node. If malicious node is found, path rater blocks that node and stops the working of malicious node.

5. EXPERIMENT RESULTS

The results are given as follows and the parameters used for simulation is given in Table.2.

Table.2. Simulation Parameters

Parameter	Value
Simulation Area	100*100(m)
Energy model	First order energy radio model, battery
Initial node energy	0.5 joule
BS position	At center point
Node distribution	Random fashion
Channel type	Wireless (via signals)
Receiving Transmit energy (E_{RX} and E_{TX})	$50*10^{-9}$
E_{DA} data aggregation energy	$1*10^{-9}$
No. of rounds	3000
Network Simulator	MATLAB
Routing Protocol	LEACH

5.1 HOMOGENEOUS LEACH

These are the simulation result of Homogeneous LEACH which has the entire sensor node having same capacity and same parameter.

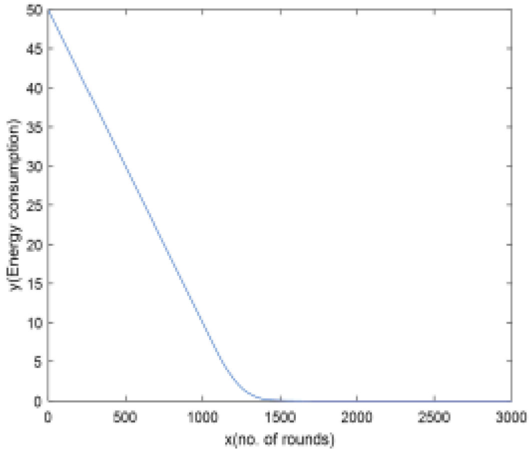


Fig.5. Energy Consumption

In Homo LEACH this the resulting graph of energy consumption whereas all energy consumed within 50 sensor node then work of the particular cluster is stop because of lack of energy.

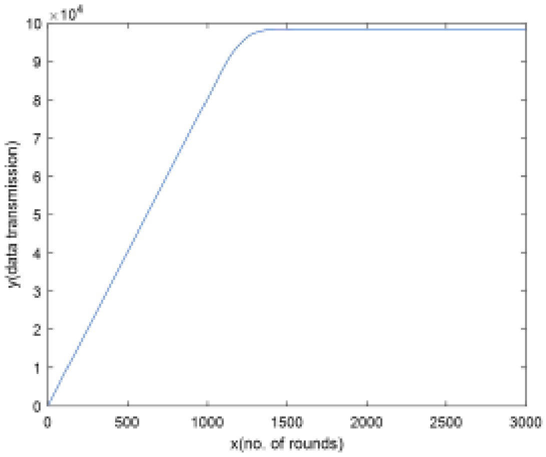


Fig.6. Data transmission

In Homo LEACH this the resulting graph of Data Transmission whereas all data transmission in between sensor node to Base station can cover the sensing area is around 10×10^4 w.r.t. particular no. of round.

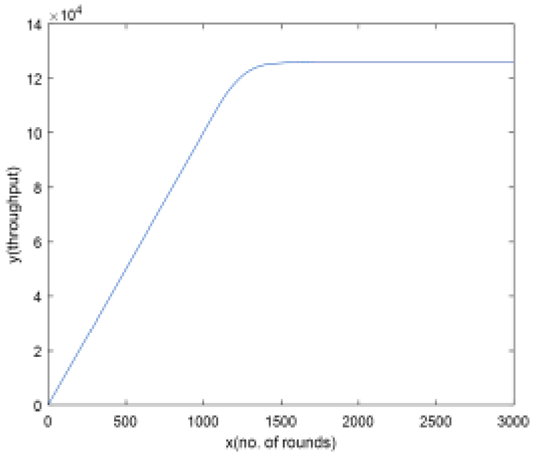


Fig.7. Throughput

In Homo LEACH this the resulting graph of Throughput nothing but successful performance and packet delivery ratio in between sensor node to Base station can cover the sensing area is around 14×10^4 w.r.t. particular no. of round.

5.2 HETEROGENEOUS LEACH

In Hetero LEACH we use two type of sensor node one is a normal and another one is advanced sensor node having different type of battery power to increase the lifespan of the particular network.

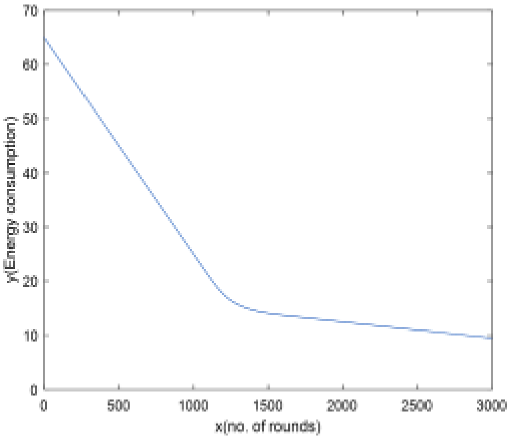


Fig.8. Energy Consumption

In Hetero LEACH this the resulting graph of energy consumption whereas all energy consumed within 70 sensor node then work of the particular cluster is going to next round as compared to Homo LEACH Hetero LEACH can exceed their work 20 sensor more because it uses advanced node ultimately it gives more throughput.

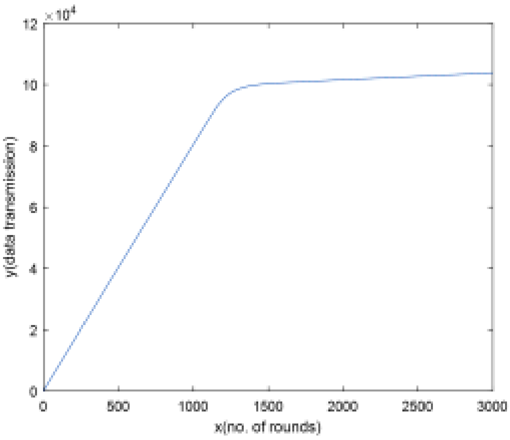


Fig.9. Data transmission

In heterogeneous LEACH this the resulting graph of Data Transmission whereas all data transmission in between sensor node to Base station can cover the sensing area is around 12×10^4 w.r.t. particular no. of round.

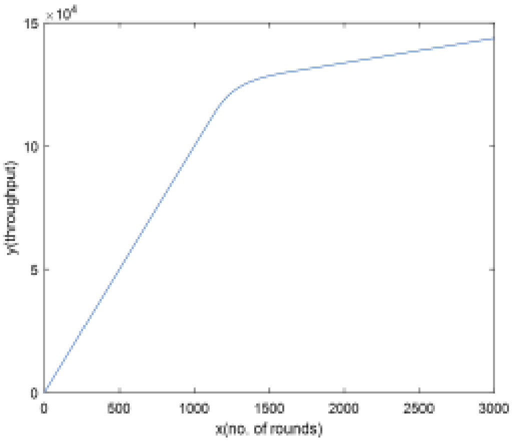
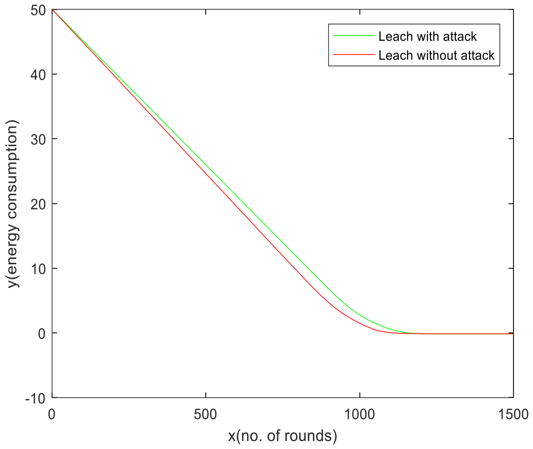


Fig.10. Throughput

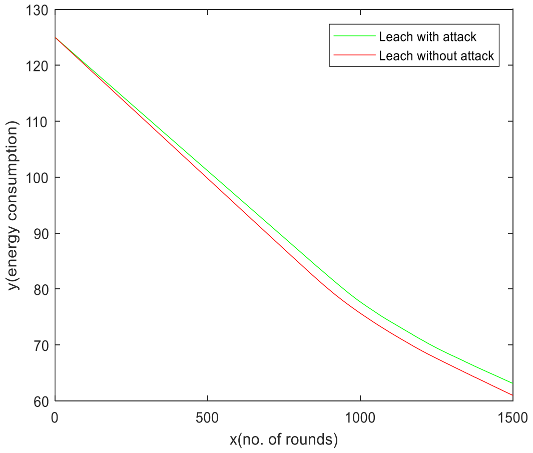
In Hetero LEACH this the resulting graph of Throughput nothing but successful performance and packet delivery ratio in between sensor node to Base station can cover the sensing area is around 15×10^4 w.r.t. particular no. of round.

5.3 LEACH WITH ATTACK

The Fig.11 shows the resulting graph of energy consumption of Homo and Hetero LEACH which is affected by sinkhole attack whereas LEACH with attack have high energy power than LEACH is no. of attack and energy in Joule.

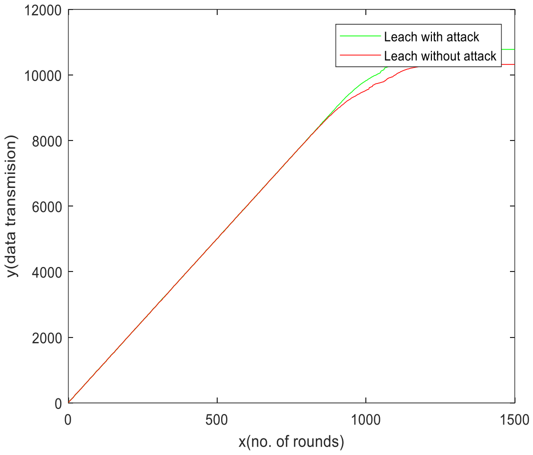


(a) Homo LEACH

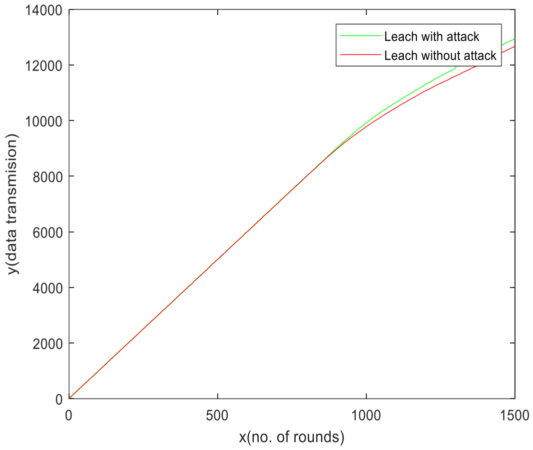


(b) Hetero-LEACH

Fig.11. Energy Consumption of Homo and Hetero LEACH with Attack



(a) Homo-LEACH



(b) Hetero-LEACH

Fig.12. Data Transmission of Homo and Hetero LEACH with Attack

The Fig.12 shows the resulting graph of Data transmission of Homo and Hetero LEACH which is affected by sinkhole attack whereas LEACH with attack have more data transmitted to the BS with minimum energy power than the LEACH without attack w.r.t. no. of rounds and energy in joule i.e. nothing but LEACH with attack is more data transmitted to the BS with minimum energy as compared to LEACH without attack.

6. CONCLUSIONS

This paper presents Homo-LEACH and Hetero-LEACH hierarchical routing protocol and clustering topology to improve network lifespan and reduce the energy consumption and sinkhole attack. How to apply sinkhole attack and how it detects and prevent by using intrusion detection technique. The result shows that the proposed system has improved performance than other existing methods.

REFERENCES

[1] M. Elshrkawey, S. Elsherif and M. Wahed, "An Enhancement Approach for Reducing the Energy Consumption in Wireless Sensor Network", *Journal of King*

Saud University-Computer and Information Sciences, Vol. 30, No. 2, pp. 259-267, 2018.

[2] M.J. Handy, M. Hasse and D. Timmermann, "Low Energy Adaptive Clustering Hierarchy with Deterministic Cluster Head Selection", *Proceedings of International Workshop on Mobile and Wireless Communication Network*, pp. 31-36, 2002.

[3] S.E.L. Khediri, N. Nasri, Anne Wei and A. Kachoury, "A New Approach for Clustering in Wireless Sensor Networks based on LEACH", *Procedia Computer Science*, Vol. 32, pp. 1180-1185, 2014.

[4] Brajesh Mishra, Sarvesh Singh Rai and Navdeep Kaur Saluja, "M-LEACH: A Modified Version of LEACH for WSN", *Journal of Emerging Technologies and Innovation Research*, Vol. 2, No. 12, pp. 82-87, 2015.

[5] P.K. Batra and K. Kant, "LEACH-MAC: A New Cluster head Wireless Sensor Network", *Wireless* Networks, Vol. 22, No. 1, pp. 49-60, 2016.

[6] Sunkara Vinodh Kumar and Ajit Pal, "Assisted-Leach (A-Leach) Energy Efficient Routing Protocol for Wireless Sensor Networks", *International Journal of Computer and Communication Engineering*, Vol. 2, No. 4, pp. 420-424, 2013.

[7] S.K. Singh, P. Kumar and J.P. Singh, "A Survey on Successors of LEACH Protocol", *IEEE Access*, Vol. 5, pp. 4298-4328, 2017.

[8] Zhenfu Ma, Guangming Li and Qingchao Gong "Improvement on LEACH-C Protocol of Wireless Sensor Network (LEACH-CC)", *International Journal of Future Generation Communication and Networking*, Vol. 9, No. 2, pp. 183-192, 2016.

[9] Shaveta Gupta and Vinay Bhatia, "GMMC: Gaussian Mixture Model Based Clustering Hierarchy Protocol in Wireless Sensor Network", *International Journal of Scientific Engineering and Research*, Vol. 3, No. 7, pp. 44-49, 2015.

[10] Ioannis Krontiris, Thanassis Giannetsos and Tassos Dimitriou, "Launching a Sinkhole Attack in Wireless Sensor Networks the Intruder Side", *Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, pp. 12-15, 2017.

[11] L. Yadav and C.H. Sunitha, "Low Energy Adaptive Clustering Hierarchy in Wireless Sensor Network (LEACH)", *Proceedings of IEEE International Conference on Inventive Systems and Control*, pp. 17-21, 2014.

[12] Ranjeeth Kumar Sundararajan and Umamakeswari Arumugam, "Intrusion Detection Algorithm for Mitigating Sinkhole Attack on LEACH Protocol in Wireless Sensor Networks", *Journal of Sensors*, Vol. 2015, pp. 1-12, 2015.

[13] Monika, Sneha Chauhan and Nishi Yadav, "LEACH-I Algorithm for WSN", *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 4, No. 3, pp. 3459-3466, 2016.

[14] Pushpender Kumar Dhiman and Shilpa Mahajan, "Clustering in Wireless Sensor Networks: A Review", *International Journal of Advanced Research in Computer Science*, Vol. 7, No. 3, pp. 198-201, 2016.

[15] Shipra Singla and Karamjot Kaur, "Comparative Analysis of Homogeneous N Heterogeneous Protocols in WSN", *International Journal of Science and Research*, Vol. 5, No. 6, pp. 1300-1305, 2016.

[16] Dinesh Singh, Parvinder Singh and Vikram Singh, "A 3-Tier Heterogeneous Secure Routing protocol for Wireless Sensor Network", *International Journal of Information Technology and Knowledge Management*, Vol. 5, No. 2, pp. 477-483, 2012.

[17] R.K. Gill, P. Chawla and M. Sachdeva, "Study of LEACH Routing Protocol for Wireless Sensor Networks", *International Journal of Computer Science and Information Technologies*, Vol. 7, No. 4, pp. 1894-1896, 2014.

[18] Jitender Grover and Shikha Sharma, "Security Issues in Wireless Sensor Network-A Review", *Proceedings of International Conference on Reliability, Infocom Technologies and Optimization*, pp. 1-6, 2016.

[19] George W. Kibirige and Camilius Sanga, "A Survey on Detection of Sinkhole Attack in Wireless Sensor Network", *International Journal of Computer Science and Information Security*, Vol. 13, No. 5, pp. 1-9, 2015.

[20] K. Johny Elma and S. Meenakshi, "Energy Efficient Clustering for Lifetime Maximization and Routing in WSN", *International Journal of Applied Engineering Research*, Vol. 13, No. 1, pp. 337-343, 2018.