https://dx.doi.org/10.24001/eec.2.4.1 *ISSN: 2456-2319*

A Secure Routing Protocol for Heterogeneous Wireless Sensor Networks

Shashikala[1], Dr Kavitha C[2]

[1]BNMIT, Department of CSE, Bangalore 70, India
[2]GAT, Department of CSE, Bangalore 70, India

Abstract*—The sensors are widely used in various applications to sense the temperature, pressure, movements in the battle field, to monitor the earthquake and so on. The sensors are so widely used because it is tiny, as sensors are tiny in nature the resource are also limited such as battery life, memory, and processing capabilities. In some of the applications, the sensor power cannot be recharged or the intruder can access the network easily. There are many heterogeneous routing protocols designed which takes care of the energy efficiency but fails to secure the network and the protocols are not using the heterogeneity of the network to the maximum extend. This work aims at providing an energy efficient routing along with securing the network from intruders. The proposed method uses the heterogeneous network to prolong the lifetime of the sensors in the network at the same time it ensures the security in the network. The proposed routing algorithm takes the advantage of heterogeneity in the network and uses a different protocol to transmit the data between the nodes. The analysis of the protocol shows how the protocol is efficient with respect to energy and security.*

Keyword— Heterogeneous, Sensor, Secure, Protocol.

I. INTRODUCTION

The advancement of the Micro-electro mechanical systems (MEMS) technology made the sensor to be widely used in various applications, because of its adopting nature, these sensors may be mobile or static. The sensors are used in various applications such as environmental monitoring, industrial monitoring, Forest Fire monitoring, Animal Habitat monitoring and so on, the sensors are used because of its low cost, and the nature of self organizes into an autonomous wireless ad hoc network, which requires little or no maintenance. These advantages lined the way for new applications where wired networks would fail or would be impractical due to the high deployment costs. The advantage of using sensors is low cost, tiny in nature, can be placed in any of the environment with little or no effort. The sensors also have the limitations, it is tiny thus it has minimum processing capabilities, and it is placed in harsh environment the battery may or may not be possible to recharge or replace which lead to low power in sensors that is sensors will not be able to transmit the data and the network lifetime also decreases due to low energy. It is prone to various attacks as it is accessible to everyone [1-4].

As there are various types of sensors are available with different capability such as battery backup, memory and processing of information, the sensor network can be classified as Homogeneous Network and Heterogeneous Network based on the type of sensors used in the network. The sensor network is said to be Homogeneous if all the sensors in the network as same processing capabilities. In Homogeneous network, the major drawback is nodes nearer to the sink will drain energy faster than the other nodes in the network in this case the other sensing nodes in the network may not be able to reach to the sink. This problem can be solved by considering the heterogeneous network. In heterogeneous networks, the different processing capability sensors are used in the same network to prolong the lifetime of the network and also to secure the network from intruders. In this proposed work we have grouped sensors with low resource capabilities as Low End Sensors (LES) and the sensors with rich in resource capabilities as High End Sensors (HES). The Fig 1.1a shows Homogeneous network with only LES and Fig 1.1b shows the homogeneous network with only HES. The Fig 1.2 is a heterogeneous network with LES and HES[4-8].

Many routing protocols are proposed for the heterogeneous sensor network. These existing routing protocols assure one or more of the following features such as stability, energy efficiency, cluster head selection, security and deployment cost.

In sensor network the network needs to be stable as each node sense the information or route the information to the sink. If any node is removed or added, still the network should guarantee coverage and connectivity throughout the network lifetime.

The routing protocols should minimize the amount of energy

https://dx.doi.org/10.24001/eec.2.4.1 ISSN: 2456-2319

consumption to transmit the data towards the sink otherwise the energy may drain out faster in the network, and network dies very early. In Homogeneous Network as all sensors are of the same processing capability so we may not be able to prolong the lifetime of the network. But in heterogeneous Network, as the processing capabilities of the sensor nodes are different the routing protocol can assign a different task to a different set of sensors. In Single routing algorithms for communication between all these sensor nodes fail to completely use the diverse capabilities of these nodes. Efficient Routing Algorithm in Heterogeneous Wireless Sensor Networks provides an optimized sensing capability, transmission range and power consumption in a Heterogeneous WSN and it can also secure against the intruder attacks such as a hello flood attack, sinkhole attack and worm hole attack, as the communication in the network is only within a small region.

The most effective routing scheme in sensor networks is normally based on the energy of the nodes. In such routing schemes the best path has the highest amount of total energy. Developing an energy-efficient routing protocol has a significant impact on the overall lifetime, performance and stability of the sensor network. The key concept is to exploit the trade-off between energy consumption and timeliness to maximize the system useful lifetime. Efficient energy conscious routing algorithms can potentially prolong the lifetime of the network.

The process of electing the cluster head uses all most 10% of the network energy. In this proposed work the heterogeneity is considered, the HES are made as the cluster head and LES will sense the data and transmit to the HES, which in turn save the energy consumption of the network and prolong the network lifetime.

As sensors die in the network, we add/replace new sensors to the network; in this process the deployment cost of the network should not be high. A mixed deployment of these nodes can achieve a balance of performance and cost of WSN. To maintain a symmetric communication, the distance between high end and low end sensor nodes cannot be larger than the maximum communication range of the low end sensor. Using an optimal mixture of many inexpensive, low capability devices and some expensive high capability devices can significantly extend the duration of a network's sensing performance. Two configurations can be achieved in a homogeneous system.

i. Less expensive least powerful conglomeration of all LES nodes.
ii. Highly expensive and more powerful conglomeration of all HES nodes.

Both these configurations do not prove to be effective for real world applications. But a heterogeneous WSN strikes a balance between cost and performance. It is cost effective and powerful as it enables faster transmission.

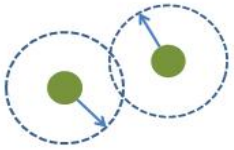

Fig 1.1a - Homogeneous Networks with LES

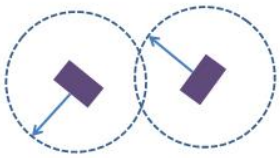

Fig1.1b Homogeneous Network WITH HES.

The heterogeneous WSN consists of sensor nodes with different abilities, such as various sensor types and communication/sensing range, thus provides more flexibility in deployment, thus a Heterogeneous sensor network can achieve a balance of performance and cost.

In sensor network the security is another important issue. The security can be provided either for the sensed data or the transmission path. The security to the sensed data can be achieved by applying the one-way hashing algorithm which requires a very minimal resource. The security to the transmission path is very tricky because the sensor nodes are deployed anywhere in the environment, and it can be accessed by anyone. The node can be compromised by the intruder and energy can be drained out from the network very fast by using a Hello flood attack, Selective forwarding attack, or DoS attack. In the proposed work the security for the transmission path is achieved[5-10].

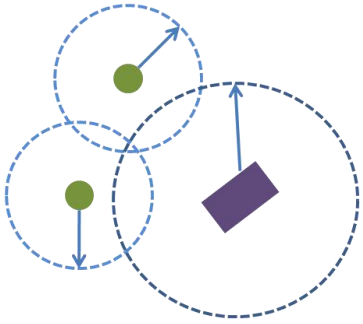

Fig 1.2 A Heterogeneous Networks showing both Low End Sensor and High End Sensor together.

https://dx.doi.org/10.24001/eec.2.4.1 *ISSN: 2456-2319*

The rest of the paper is organized as second session related work gives an overview of the existing heterogeneous routing protocols. The third specifies the detail working of the proposed routing protocol and finally in the performance analysis the SRHWSN routing protocol analysis is discussed with graph.

II. RELATED WORK

Many protocols are proposed to minimize energy consumption and maximize the sensing capability and transmission range of sensor nodes. A homogeneous sensor network consists of identical nodes, while a heterogeneous sensor network consists of two or more types of nodes (organized into hierarchical clusters). LEACH is used as the representative for the single hop homogeneous network and a sensor network with two types of nodes as a representative for the single hop heterogeneous network. For multi-hop homogeneous networks (nodes use multi-hoping to reach the cluster head), a multi-hop variant of LEACH (M-LEACH) is proposed and analyzed. The results show that M-LEACH has better energy efficiency than LEACH in many cases [1].

The ProHet: a Probabilistic routing protocol for Heterogeneous sensor networks, which can handle asymmetry links well and work in a distributed manner using local information with low overhead and assured delivery rate. It has two parts: the preparation part, which includes identifying neighbor relationships and finding a reverse path for an asymmetric link, and the routing part which includes selecting nodes, forwarding messages and sending acknowledgements. The protocol differentiates the diverse transmission ranges of sensors and takes advantage of the asymmetrical links to achieve assured delivery rate [4].

Chun-Hsien Wu et al has proposed the method to deploy and control the topology in heterogeneous sensor nodes with different communication and sensing range. It is based on the irregular sensor model used to approximate the behavior of sensor nodes. Besides, a cost model is proposed to evaluate the deployment cost of heterogeneous WSN. This method can achieve higher coverage rate and lower deployment cost for the same deploy able sensor nodes [5].

The Redundancy Management of Heterogeneous Wireless Sensor Networks (HWSNs), utilize the multi-path routing to answer user queries in the presence of unreliable and malicious nodes. The key concept is to exploit the trade-off between energy consumption vs. the gain in reliability, timeliness, and security to maximize the system useful lifetime. It develops a novel probability model to analyze the best redundancy level in terms of path redundancy and source redundancy, as well as the best intrusion detection settings in terms of the number of voters and the intrusion invocation interval under which the lifetime of a HWSN is maximized. It applies the analysis results obtained in the design of a dynamic redundancy management algorithm to identify and applies the best design parameter settings at run time in response to environmental changes, to maximize the HWSN lifetime [6].

In wireless sensor networks, energy constraints of each node directly affect the lifetime of wireless sensor networks; therefore, how to save energy is an important issue. In practice, due to environmental differences of sensor nodes, different tasks are assigned to each node, and the resulting heterogeneous wireless sensor network (HWSN) is more likely to cause inconsistency in network energy loads, thus, reducing effective lifetime. The study presents a re-clustering algorithm with energy awareness in HWSN. The algorithm considers some key factors that include residual energy, distance, and communication cost and then creates an appropriate re-clustering threshold for each cluster head to save energy consumption [8].

Energy Efficient Stable Election Protocol (EE-SEP) is proposed which uses two different thresholds for HES and LES which is a good impact on stability, network life time and cluster heads formation in every round when compared to LEACH and SEP but as cluster head is elected every round the energy consumption is more [10].

V.T.Kesavan and et al, proposed a secure cluster based routing for WSN with dynamic key management. In this method the cluster head is elected based on node degree, distance to sink, node velocity and virtual battery power. The dynamic key is generated based on the location, node degree and batter power, this key are further used to achieve the integrity and confidentiality. The routing algorithm has to take care of the security at the time of cluster formation and later to the data. The node as mobility, so the node moves from one cluster to another, then, the process is done again and again which consumes more energy of the nodes. It is also prone to various attacks such as compromised attack. The intruder can send is false location and node degree to calculate the dynamic key generation and the intruder can read all information in the network [11].

Songhua Hu and et al, has proposed the cluster based optimization algorithm for WSN. The heterogeneity is considered, the low energy sensors (LES) nodes are deployed randomly and high energy sensors (HES) are deployed artificially in the center. The LES sense information and routes to the CH or HES with multi hop. Even those the multi hop is energy efficient, but the nodes near the sink will drain-out energy earlier and they will not be able to forward the

https://dx.doi.org/10.24001/eec.2.4.1 ISSN: 2456-2319

data to the sink that is the number of isolated nodes will be increased in each cluster [12].

We propose "A secure Routing for Heterogeneous Wireless sensor Network" and it is energy efficient, algorithm that works its way through an HWSN that contains a limited number of fixed high end sensor nodes and densely populated low end sensor nodes. The proposed protocol implements different techniques to transmit the data between Low end sensors to High End sensors and from High End sensors to sink. The proposed method is composed of two routing techniques.

III. A SECURE ROUTING FOR HETEROGENEOUS WIRELESS SENSOR NETWORK (SRHWSN).

We propose SRHWSN an efficient routing algorithm that works its way through an HWSN that contains a high end sensor node placed with equi-distance in the sensory region and densely populated low end sensor nodes. The SRHWSN is a secure and energy efficient as it uses two different routing protocol to transmit the information. The SRHWSN has three different phases to make it secure and energy efficient.

The first phase is Network Deployment phase, in this the LES are placed randomly and the HES are placed in a predefined pattern generated using the Algorithm-1.1. The major advantage of using the Algorithm-1.1 is, it lessens the isolated nodes from network as it makes sure that the HES is distributed equally throughout the sensing region. In the second phase the data is sensed by the LES and apply the one way hash function for data and forwards toward the sink via LES and then to HES using two different routing protocols. In the third phase the hashed value is verified against the original data and then forwarded to the sink. To achieve these operations, we have assumed the parameters as listed in the Table.I for simulation.

Table.I: Network Parameters

Parameter	HES	LES
Radio Range	300m	150m
Initial Energy	200J	50J
Transmission Energy	0.005J	0.002J
Receiving Energy	0.003J	0.001J
Minimum Energy	0.005J	0.002J
Area	500m	500m

✓ Network Deployment

The Network is a heterogeneous containing the Low End Sensors (LES) and High End Sensors (HES). The LES and HES communicate over the sensing area. The number of HES and LES in the sensing region is given by the Equation (1) and (2).

$$N_h = N_n * \alpha \quad \ldots\ldots\ldots\ldots (1)$$

$$N_L = N_n - N_h \quad \ldots\ldots\ldots\ldots (2)$$

Where α gives is the ratio for the number of HES in the sensing region, the value of α decreases as the number of node increases in the sensing area network. The value of α ranges between $0.1 \leq \alpha \leq 0.2$ [11], N_h is the number of HES nodes in the network, $N_L$is the number of LES nodes in the Network and N_n is the total number of sensor nodes in the network.

The HES are deployed across the sensing area to provide an efficient routing for the data. These nodes are placed in the network area based on the pattern shown in the Fig 1.3 the position is calculated based on the number of HES in the network. This pattern takes care of even distribution of HES that is there is no two HES overlap in radio range.

The pattern in the Fig 1.3 can be applied for any number of HES node. For example, if Nh =5 then the function calls N_h with value 4 and 1, similarly if N_h =19, then the function is called recursively in the first iteration with N_h =19, then with N_h set to (19-8), (11-1) then finally with N_h =3. Each time the recursive function is called the sensing region boundary is decreased. As the number of HES increases in the network the number of isolated nodes decreases in the sensing region.

As the number of isolated nodes decreases the lifetime of the network is high, because the number of nodes participating to forward the data to HES is more. The number of nodes sensing is also more which improves the accuracy of the data. The node location is stored only in its ancestor and in successor node this also makes the routing protocol to secure the path in the network. The LES are deployed in the sensing area randomly to achieve the maximum data transmission from the sensing region with minimum energy consumption. As sensor nodes are self organizing and self configuring. The LES will send the control packet with its location, residual energy to all its nodes, which lies within the radio range of it. This helps LES to identify its neighbor LES and HES, which is very close to it. The control packet is sent periodically to ensure that its neighbor nodes are well in its place. This also helps to identify the intruder as the location is shared among all its neighbor nodes.

https://dx.doi.org/10.24001/eec.2.4.1 ISSN: 2456-2319

Algorithm 1.1 HES_Generate_Pattern(N_h)
Input: Xmin, Ymin, Xmax, Ymax, N_h
Output: For each N_h the X, Y coordinates are generated within the region (Xmin,Ymin) to (Xmax,Ymax)
Description: The HES_generatePattern algorithm is used to distribute the HES node across the sensing region so that we can minimize the isolated nodes in the network.
Switch (N_h)
Case 1:
(X,Y)= ((Xmax+Xmin)/2, (Ymax+Ymin)/2)
Return (X,Y)
Case 2:
P1 = (Xmax,Ymax)
P2 = (Xmin,Ymin)
Return P1,P2
Case 3:
HES_Generate_Pattern (1)
HES_Generate_Pattern (2)
Case 4:
P1 = (Xmax,Ymax) ; P2 = (Xmin,Ymin) ; P3= (Xmax,Ymin) ; P4=(Xmin,Ymax)
Return P1,P2,P3,P4
Case 5:
HES_Generate_Pattern (1)
HES_Generate_Pattern (4)
Case 6:
HES_Generate_Pattern (4)
HES_Generate_Pattern (1)
Case 7:
HES_Generate_Pattern (4)
HES_Generate_Pattern (3)
Case 8:
HES_Generate_Pattern (4)
P1 = (Xmax+Xmin)/2,(Ymin+Ymin)/2 ;
P2 = (Xmin+Xmin)/2,(Ymin+ymax)/2 ;
P3= (Xmax+Xmin)/2,(Ymax+Ymax)/2 ;
P4= (Xmax+Xmax)/2,(Ymin+Ymax)/2;
Default:
Xmin = Xmin+D
Ymin = Ymin+D
Xmax=Xmax-D
Ymax=Ymax-D
HES_Generate_Pattern (Nh-8)
End Switch

(a) (b) (c) (d) (e) (f)

Fig 1.3 The basic patterns to place the HES nodes in the sensing area to avoid the overlapping of the HES (a) When N_h=1, (b) N_h=2, (c) N_h=3 (d) N_h=4, (e) N_h=6, (f) N_h=7

✓ Routing in a Heterogeneous network

The node updates the neighbor list in it, then the node as to route the data towards the sink in an efficient way. The routing within the network is either between

i. Routing between Source and HES
ii. Routing between the Sink and HES

i. Routing between Source(LES) and HES

This algorithm finds the shortest path between LES and HES. In this method, it finds an alternative path to send the data from the source to the destination. The simple path-loss model called free space model is used with an, assumption that there is no obstructions between transmitter and receiver. The free space model path loss (PL) is proportional to the square of the distance between transmitter and receiver and is given by equation 3.

$$PL = (1/d)^{\alpha} \quad \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

Using this model we can express the receiver power at distance 'd' as

$$Pr = P_0(d_0/d)^{\alpha} \quad \ldots\ldots\ldots\ldots\ldots\ldots(4)$$

Let the power consumed for single hop be

$$Pm = P_1(d_0/d)^{\alpha} \quad \ldots\ldots\ldots\ldots\ldots\ldots..(5)$$

Similarly for the 2-hop, 3-hop, 4-hop, ……, n-hop the power is consumed

$$P_n = n.\frac{P1}{n^{\alpha}} \quad \ldots\ldots\ldots\ldots\ldots\ldots..(6)$$

From the equation 6 it can be noted that the multi-hop transmission is better than the single hop transmission. But if the receiver power Pr is not ideal then the above equation changes to the equation (7)

$$P_n = n.\left[\frac{P1}{n^{\alpha}} + Pr\right] \quad \ldots\ldots\ldots\ldots\ldots\ldots (7)$$

$$Pr = \frac{n^{\alpha-1}-1}{(n-1)n^{\alpha-1}} P1 \quad \ldots\ldots\ldots\ldots\ldots\ldots (8)$$

From the equation (8) it can be noticed that the multi-hop is efficient if Pr is less than the transmission power otherwise the multi-hop is not efficient. Considering this scenario in our method we have restricted the number of hops required to transmit the data in the network from LES to HES.

As the number of multi hop nodes is limited due to this the power consumption is also almost constant to find the neighbor nodes. By taking this advantage it is possible for us to find 'n' alternative path between LES and HES.

Let the alternative path generated are P1, P2, P3, …….. , Pn and these paths are disjoint in nature, that is

https://dx.doi.org/10.24001/eec.2.4.1 ISSN: 2456-2319

$P1 \cap P2 \cap P3 \cap P4 \ldots\ldots\ldots \cap Pn = \Phi$. ……(9)

The advantage of having a disjoint path in the network is if one path fails the other path can still send the data. The other advantage is if any ode is compromised that can be detected and prevented from the network to transmit the data to the HES. A simple algorithm to find the path from LES to HES is given in the Algorithm 1.2.

Consider the Fig 1.5 for LES to send data to HES. The source has three alternative paths to reach the nearby HES. In the first path, if the intruder drops or modify the message the HES compares the data received from path 1 with the data received from the other two paths if the data received from path2 and path 3 is same but in paths 1 it is different, then HES considers that the path is misbehaving and informs to the source not to send data via that path1.

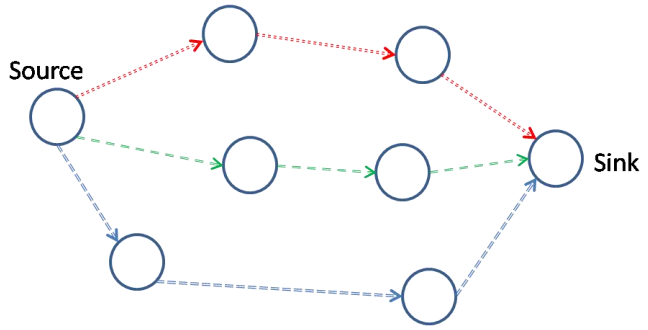

Fig 1.5 Showing the alternative path from Source (LES) node to Sink (HES) nodes

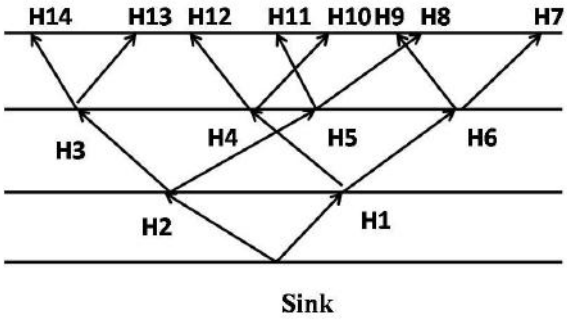

Fig 1.6 The branching random walk

i. Routing between the Sink and HES

In this phase the data is transmitted from HES to Sink. The low end sensor node transmits the packets to the nearest high end sensor node. This in turn has to be routed to the sink.HES as to transmit the data to the sink. The sink will initially send the control packet to all HES to send its identification such as Node id, Location, residual energy, upon receiving this information, the sink estimates the distance from sink to all other HES in a network using Euclidean distance as given in the equation (10).

Euclidean distance = $\sqrt{(x1 - x2)^2 + (y1 - y2)^2}$ …(10)

Let N_k is the sink and H1, H2, H3, ……N_h is the number of HES in the network. The random walk constructs the tree based on the sink establishes the path to all HES in the network using the equation (11) and (12) recursively.

N_{kL} = Small[(h1, h2, h3……..,N_h),1] …….. (11)

N_{kR} = Small[(h1, h2, h3……..,N_h),2] ……. (12)

The Euclidian distance is calculated for the left child and for right child using the HES information available in the sink node, the process continues until all HES are reachable from the sink. The sink updates predecessor and the successor node information from its mater routing table to all HES in the network. The branching random walk is based on Euclidian distance and it is constructed as shown in fig 1.6.

In the master routing table for the root node, the parent Id and the Node Id is same. The nodes which do not have either or both left child or the right child the value set is -1 to make sure that it is a leaf node. These HES acts as a Cluster Head in the network and LES will communicate with these HES. The routing protocol does not elect the cluster head after few rounds rather by taking the advantage of the heterogeneity, the HES are made as cluster head. As the cluster head is no elected again and again the power consumption for the same is not required.

Also the HES will store only the parent and the child node id and its location at it has no idea about the other HES in the network. The intruder will not be able to get into the other nodes. The tree constructed by using the random walk is shown in the Fig 1.7 for the number of HES equal to 5. The corresponding master routing table is shown in Table-II.

https://dx.doi.org/10.24001/eec.2.4.1 ISSN: 2456-2319

Algorithm 1.2 Finding the shortest path from LES to HES

Input: Number of nodes *N*
Output: Path array *path*
Description: For every LES, find the shortest path to reach HES with the maximum of two hops

for *i* =N_h to *N* **do**
repeat
Rearrange the distance of the nodes in ascending order for
every i^{th} row
Find the node id of the nearest node
until N_h is found
Update the *path* to sensor node data structure
end for

Algorithm 1.3 Tree Data Structure

Input: *Reachability Matrix, Visited Array*
Output: *Tree*
Description: Produces the tree representation for the set of nodes containing Base Station and all HES.
Euclidian_Distance (Nk)
Initialize sink node as root
Update the tree table
repeat
N_{kL} = SMALL(H1,H2,H3,……Nh,1)
N_{kR} = SMALL(H1,H2,H3,……Nh,2)
Left_childe= N_{kR}
Right_child = N_{kR}
Update the visited for Left Child and Right Child nodes
Nk= N_{kL}
Euclidian_Distance (Nk)
Nk= N_{kR}
Euclidian_Distance (Nk)
until all nodes are visited

Table-II Master routing Table illustration

Node ID	Parent Node ID	Left Child	Right Child
5	5	4	2
4	5	0	1
2	5	3	-1
0	4	-1	-1
1	4	-1	-1
3	2	-1	-1

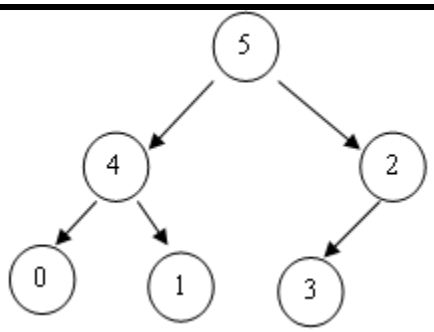

Fig 1.7 Tree structure for HES=5 using master routing table

ii. Network Integrity

In the SRHWSN routing protocol we assure that the routing protocol assures the data Integrity and data confidentiality.
The Data Integrity is achieved by using a one way hash function. We assume that the key is distributed at the time of network deployment. The sensor node senses the data and stores the data along with the time stamp for small duration. The LES on receiving the request from HES, it will apply the hash function on data along with the time stamp and the original data is transmitted by the source to the HES.
At HES, on receiving the data it applies the hash function on data and compares the newly generated hash value with the one received from the LES. If the hash values are same the data is accepted and stored in the HES. This ensures that the data is not modified and achieves the data integrity.
The data confidentiality is to make sure that the data stored on the sensors are protected against the intruders. In this routing protocol the data is stored in the LES for a small duration data, data keeps updating in the LES.As the data are updated by the LES periodically, there are two situations in the routing protocol where the data confidentiality is achieved.

- The sensed data is transmitted, then the intruder modifies the data,
- The intruder as modified the data, but LES will not receive the request from HES and it updates he data with new data sensed which also updates the data modified by the intruder.

The data confidentiality is achieved in the above cases by the routing protocol because the LES refreshes the data in random intervals.

IV. Performance Analysis

The simulation results show that the SRHWSN is a secure and energy efficient routing protocol. For the simulation the network sensing region is considered is 500m X 500m. The fig 1.8 shows the path in the densely populated sensor nodes in the network. In fig 1.8 the circles represent the LES whose positions are randomly generated and the

https://dx.doi.org/10.24001/eec.2.4.1 *ISSN: 2456-2319*

squares represent the HES whose positions are fixed. LES that generate packets find an optimal path to reach the nearest node. The lines represent the routing path between the LES and the nearest HES to that node. The only one path from LES to HES is shown in the fig 1.8 but actually it constructs a three disjoint paths with maximum hop count of 3. On receiving the packets, the HES forward the packets in accordance to the tree data structure until it reaches the Base Station.

The routing protocol is secured its path from various attacks such as vampire attack, Hello Flood Attack, Worm Hole Attack and Sink Hole Attack.

In Vampire attack, the data is routed to the sink through a long path rather than with a short path, to simply drain out the energy from nodes. But in our routing protocol the maximum number of hop count is restricted to three, in each node before forwarding the count in decremented and when the count reaches to zero the packet is discarded, which in turn make sure that the intruder will not be able to route the packet for long path.

In Hello Flood Attack, the intruder will flood the network with more packets so that the nodes will transmit and drain out with the energy, but as the number of hop count is set to a maximum of three, the packets are discarded when the count reaches zero. And also if in case the packets are flooded and it reaches to the HES, the HES will monitor the sensor node continuously and it sends messages to all its neighbors indicating that the node an intruder and all the sensors should stop transmitting or forwarding the data through it. The node monitoring is done by the HES but not by the LES thus the lifetime of the sensor nodes can be improved.

In wormhole attack, the two compromised nodes will form a tunnel and diver all traffic from one end to the other end. This attack is performed on the HES rather than on LES because the LES is volatile in nature, but HES is non-volatile and also it stores the information in it, but to attack the HES the intruder requires rich resource and it may not be cost effective.

In sinkhole attack, the intruder will send the false message as it has more residual energy, and through it the HES can be reached with less cost to all nodes in the network. But as the network is heterogeneous it is difficult for the intruder to impersonate in the network and it may not be cost effective.

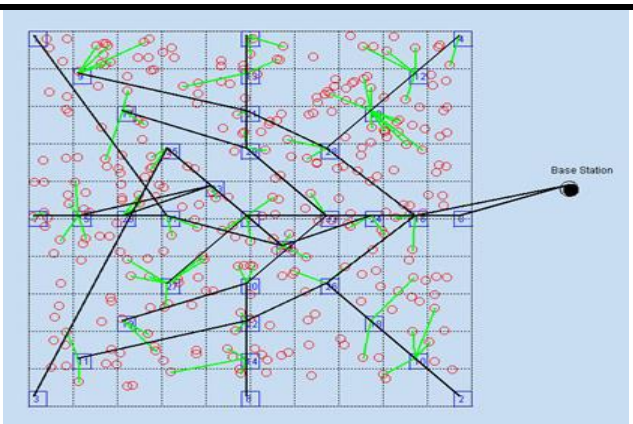

Fig 1.8 Network shows the deployment of the sensor Nodes

✓ **Residual energy of the network.**

The residual energy of the network is the energy remaining in the network after iteration. The fig 1.8 shows the residual energy of the network. The Energy in the network is calculated using the equation (13).

Residual Energy = Total Energy of all nodes in network – consumed energy ……. (13)

Where, consumed energy is the sum of energy consumed during transmission and reception. The Energy for Low End Sensor nodes is as shown in Fig. 1.9. It can be inferred from the graph that given the any number of nodes, the energy remains almost constant irrespective of the time for which the simulation is run.

✓ **Throughput v/s number of nodes**

The Fig 1.10 shows the throughput of the network in the assumed simulation. The Throughput is the time towards the completion of sending data to the destination. In SRHWSN routing protocol the throughput is almost constant for the number of nodes verses the simulation time. When the number of nodes in the network is less the throughput also varies, but as the number of nodes is increasing the throughput becomes almost constant because the HES are are more and it is evenly distributed in the network without overlapping by using the pattern designed for the network. When HES is not distributed evenly then the through but is not constant.

https://dx.doi.org/10.24001/eec.2.4.1 *ISSN: 2456-2319*

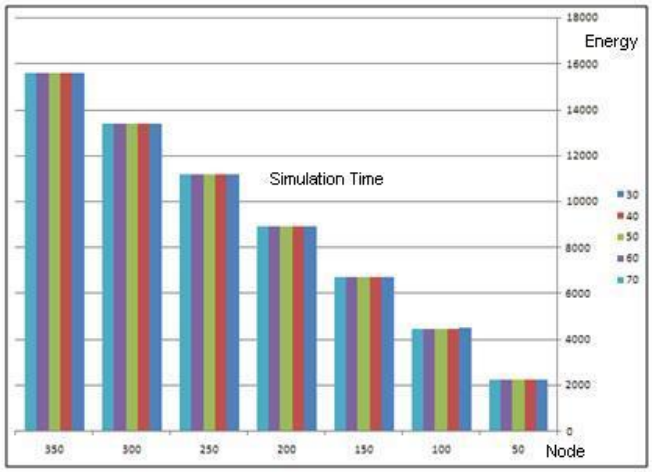

Fig1.9 The residual Energy of the network with the parameter Number of Nodes in the network, Simulation Time and the residual energy.

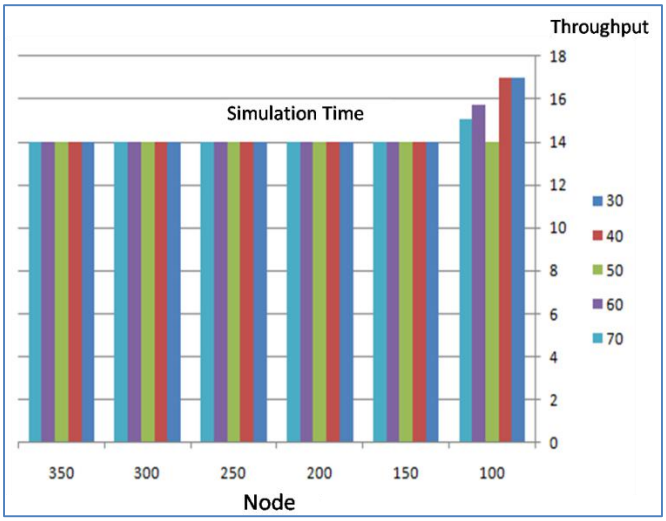

Fig 1.10. Throughput of the network with the parameter simulation time, Number of Nodes and throughput value

V. CONCLUSION

In this proposed routing protocol, we have considered the heterogeneous network with the LES and HES to transmit the sensed information securely from the source to the sink with minimum energy. The system architecture proposed exploits the advantages of these nodes and their placement in the network. The proposed system proves to be efficient as it gear with two routing protocol algorithms and it does not form a cluster in it which saves almost 16% of the network energy towards electing the cluster head periodically. The first algorithm finds the shortest paths from the transmitting sensed data from low end sensor node to one high end sensor with a maximum of three hop count. And the second algorithm computes the minimum spanning tree for the high end sensors with base station as the root. As two routing protocols we are used to transmit the data from sensing region to Sink, it also secures the network path from various attacks like a vampire, sink hole, warm hole and Hello flood attacks. This routing protocol can be further enhanced to generate infinite disjoint paths with increasing the maximum hop count. The overall performance of the system is analyzed based on energy, throughput.

REFERENCES

[1] Mhatre, V., Rosenberg, C. "Homogeneous vs. heterogeneous clustered sensor networks: A comparative study". 2004 IEEE International Conference on Communications (ICC'04), Paris, France, Jane, 2004, Vol. 6, pp. 3646–3651.

[2] Mini, S. ,Udgata, S.K. , Sabat, S.L. "Sensor Deployment and Scheduling for Target Coverage Problem in Wireless Sensor Networks ".IEEE Sensors Journal. Vol. 14, No. 3, March 2014, pp. 636-644.

[3] N. Javaid, S. N. Mohammad, K. Latif, U. Qasim, Z. A. Khan, M. A. Khan. "HEER: Hybrid Energy Efficient Reactive Protocol for Wireless Sensor Networks" . Electronics, Communications and Photonics Conference (SIECPC), 2013 Saudi International.

[4] Xiao Chen, Zanxun Dai, Wenzhong Li, Yuefei Hu, Jie Wu, Hongchi Shi, and Sanglu Lu. "ProHet: A Probabilistic Routing Protocol with Assured Delivery Rate in Wireless Heterogeneous Sensor Networks". IEEE Transcations on Wireless Communications, Vol. 12, No. 4, April 2013. pp. 1524-1531.

[5] Chun-Hsien Wu and Yeh-Ching Chung, "Heterogeneous Wireless Sensor Network Deployment and Topology Control based on Irregular Sensor Model", Advances in Grid and Pervasive Computing ,Volume 4459, 2007.

[6] Hamid Al-Hamadi and Ing-Ray Chen "Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks" IEEE Transactions on Network and Service Management, Vol. 10, No. 2, June 2013.

[7] Mohammad Hammoudeh and Robert Newman "Adaptive routing in wireless sensor networks: QoS optimisation for enhanced application performance" Elsevier inffus 2013.

[8] Hung-Chi Chu, Meng-Hung Chi and Fang-Lin Chao "An Energy-Aware Reclustering Algorithm in Heterogeneous Wireless Sensor Networks". R.Chen (ed.), 2011 International Conference in Electrics, Communication 1077 and Automatic Control

https://dx.doi.org/10.24001/eec.2.4.1 *ISSN: 2456-2319*

Proceedings, LLC 2012, pp. 1077-1084

[9] Wu Yangbo, Zou Donglan, and Li ShuLiang "A Modified Transport Protocol for Heterogeneous Wireless Sensor Networks". 2013 Intelligence Computation and Evolutionary Computation, AISC 180, pp. 875–879.

[10] T.Venu Madhav and N.V.S.N. Sarma "Energy Efficient Cluster Routing Protocol for Heterogeneous Wireless Sensor Networks". CNC 2012, LNICST 108, pp. 452–455, 2012.

[11] V.Thiruppathy Kesavan and S.Radhakrishnan "Secure clustering and routing for heterogeneous mobile wireless sensor networks with dynamic key management" Journal of Experimental and theoretical Articicial Intelligence-2015.

[12] Songhua Hu and et al " A multihop heterogeneous cluster based optimization algorithm for wireless sensor networks" Springer Wirless Networks pp-57-65 2015.