Asian Journal of Information Technology 15 (3): 437-447, 2016
ISSN: 1682-3915

SEE-AMRoute Routing Control Protocol in Green Wireless Sensor Network by GIHBR Algorithm

[1]T. Akila and [2]P. Uma Maheswari
[1]Department of Computer Science and Engineering, Mahendra College of Engineering,
Salem 106, TN, Anna University, Chennai, India
[2]Anna University, Coimbatore, India

Abstract: Wireless sensor network is an influential factor and play an extensive role now a days. High Energy utilization is the major obstacle in WSN and it may pernicious to human being. "Green" has now a days become a well-known concept and an appealing trend. Efforts to reduce energy consumption are now important topics in many aspects of our daily life. Green wireless sensor network mainly focuses on energy efficiency improvement aiming at the realization of sustainable or battery less operation of the networks. In our research, green wireless sensor network is used as a network environment which saves network energy usage by embracing Periodic data reporting and absence of timestamp synchronization. This study exploits Green Indemnity Honey Bee Routing Algorithm (GIHBR). The AMRoute is the multicast routing protocol that achieves the robustness due to its tree structure over an underlying mesh structure. But, this protocol is less efficient due to loop formations in multicast tree and does not consider the node's energy level while forming the mesh and tree creation. To solve this problem, this study offers GIHBR principles to present a new routing protocol called SEE-AMRoute. The GIHBR Routing algorithm works in a honey bee technique which consumes lesser amount of energy compared with other technique. To afford reliable network lifetime and node authentication for security, indemnity technique such as threshold based link break detection mechanism, Optimized Homomorphism Signature algorithm has been developed. Hereby, using extensive simulation results, the proposed scheme achieves minimum energy consumption, high network lifetime, less delay, reduced overhead and increase delivery ratio.

Key words: GWSN, GIHBRA, AMRoute, energy-aware, indemnity, optimized homomorphism signature

INTRODUCTION

Wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions. A sensor network consists of multiple detection stations called sensor nodes, each of which is small, lightweight and portable.

Every sensor node is equipped with a transducer, microcomputer, transceiver and power source. The transducer generates electrical signals based on sensed physical effects and phenomena. The microcomputer processes and stores the sensor output. The transceiver receives commands from a central computer and transmits data to that computer. The power for each sensor node is derived from a battery. The WSNs were initially designed to facilitate military operations but its application has since been extended to health, traffic and many other consumer and industrial areas. A WSN consists of anywhere from a few hundreds to thousands of sensor nodes. The size of the sensor nodes can also range from the size of a shoe box to as small as the size of a grain of dust. As such, their prices also vary from a few pennies to hundreds of dollars depending on the functionality parameters of a sensor like energy consumption, computational speed rate, bandwidth and memory.

Green wireless sensor network: According to a report by the Energy Information Administration, Many organizations today are speaking openly about a desire to

Corresponding Author: T. Akila, Department of Computer Science and Engineering, Mahendra College of Engineering, Salem 106, TN, Anna University, Chennai, India

operate in a "green" manner, publishing principles for environmental practices and sustainability on their corporate web. In this study, we focus on reduction in energy consumption over the full equipment life cycle as the prime motivator for "green" application design with energy reduction as the best measure of "greenness". Our sole motivation is reducing energy consumption without regard to economic impact.

Since, today's wireless terminals are typically equipped with multiple network access interfaces such as Bluetooth, WI-Fi and cellular networks. User terminals cooperating with each other in transmitting their data packets to the Base Station (BS) by exploiting the multiple network access interfaces, called inter-network cooperation. The energy consumption of these interfaces and for packet transmission is high. Green wireless sensor network, which emphasizes on energy efficiency, is thereby attracting more and more attention and becoming the main trend for future wireless network design. The major object of our research is to develop energy-efficient architecture, protocols and techniques for robust and secure wireless networks.

Need for green wireless sensor network: Periodic data reporting with the periods set by the users, permits less energy use overall and avoids energy spikes such as those which are commonly found with event-driven data reporting. For example, in the presence of an event, sensors utilized large amount of energy often reporting redundantly. In contrast, the GWSN outlined here supports periodic reporting and a corresponding amount of energy is saved, depending on the period used but by having a dynamic, user-specified periodic reporting rate, overall energy consumption is reduced a variable amount.

Absence of timestamp synchronization permits the sensors to be considered autonomous systems. As a result, there is no need for blast communications to all sensors to synchronize them and the returning responses from each sensor with the resulting REQ/RESP pairs until the SYN process has completed. Depending on the frequency of reporting and the energy consumption of the sensors, this can result in a savings of up to 50% of the network energy usage which can be used to report sensor reading, rather than expending energy on the management of a central synchronized clock.

Literature review: Yuea *et al*. (2012) study an Energy Efficient and Balanced Cluster-based Data Aggregation algorithm (EEBCDA) is introduced. It works by dividing the network into rectangular grids with unequal size and makes cluster heads rotate among the nodes in each grid respectively, the grid whose cluster head consumes more energy has more sensor nodes to take part in cluster head rotation and share energy load, by this way, it is able to balance energy dissipation. This increases the network lifetime, energy efficiency and balanced extent of energy dissipation.

Poonguzhali (2014) study an Enhanced Forward Aware Factor-Energy Balanced Routing Method (EFAF-EBRM) based on Data aggregation technique is used. It has some key aspects such as a reduced number of messages for setting up a routing tree, maximized number of overlapping routes, high aggregation rate and reliable data aggregation and transmission. The EFAF-EBRM is compared with FAF-EBRM and LEACH and the results show that proposed method outperforms which balances the energy consumption, prolongs the network function lifetime and provides the best aggregation quality.

Chen *et al*. (2009) study mathematically calculating the traffic load of a node is difficult in a wireless sensor networks. An analytical model for estimating the per-node traffic load in a multi-hop wireless sensor network is introduced. The sensor nodes periodically sense the environment and forward the collected samples to a sink using greedy geographic routing. It works by calculating, per-node traffic load can be used to estimate the energy consumption of each sensor node given that the energy expended in transmitting packets makes up a significant portion of a node's energy budget. Latter, it can then be used to predict the operational lifetime of the network which is an important criteria for designing sensor networks. Further, the per-node energy consumption derived from our analysis can be useful in identifying hotspots in the network, i.e., regions where sensor nodes are expected to drain their energy at a faster rate (due to higher traffic load). Excluding these nodes other nodes traffic load is also calculated which is used to calculate the energy efficiency of the nodes in the networks. This ignorantly leads to the designing of a network in an efficient way.

Sahoo *et al*. (2013) study the honey bees mating process is introduced which is a typical swarm based approach where the search algorithm is motivated by the process of true honey bees mating. It presents a trust based secure and energy competent clustering method in wireless sensor network using honey Bee Mating Algorithm (LWTC-BMA). Moreover, it projected a pragmatic energy consumption model for exact calculation of network life span. The proposed LWTC-BMA prolong the life time of the network by depriving malicious nodes to become a cluster head. The results have also outperformed the most popular LEACH and other Honey bee based clustering (TBCMA) in terms of memory requirement, total life time and communication overhead.

Aweya (2013) study the Architecture Servo Algorithm and Phase-Locked Loop (PLL) method is used for implementing differential clock recovery over packet networks. Timing transfer and recovery over a packet network is a serious problem in the networks. Where the nodes should be in on state all the time to receive and send the packets moreover asynchronous and timing transfer capability is not embedded which consume more energy during transmission. A new mapping function is also developed for mapping the loop filter outputs into appropriate control values for driving the analog control oscillator at the receiver PLL by synchronizing the timing the energy consumption will be less.

Cheng *et al*. (2011) study a decentralized clustering algorithm for wireless sensor networks based on the structure of social insect colonies is introduced. Universally, clustering reduces the consumption of energy in the network. The structural organization of social insect colonies, an algorithm has been derived for forming and maintaining clusters in a wireless sensor network. The result performance shows that the algorithm is robust to the distribution of sensor nodes and increases the network life time.

Zhang and Shen (2010) study Energy-efficient Beaconless Geographic Routing (EBGR) is introduced. This can provide loop-free, fully stateless, energy efficient sensor to sink routing at a low communication overhead without the help of prior neighborhood knowledge. The EBGR, works by calculating each node's ideal next-hop relay position on the straight line toward the sink based on the energy-optimal forwarding distance and each forwarder selects the neighbor closest to its ideal next-hop relay position as the next-hop relay using the Request-To-Send/Clear-To-Send (RTS/CTS) handshaking mechanism. By this algorithm optimal path is measured and packets are transmitted with less energy consumption.

Thayananthan and Alzranhi (2014) study the nodes in the sensor networks are battery powered, improving the network lifetime and energy efficiency is the problem normally faced in networks. Enhancement of energy conservation technology is introduced it is a combination of routing and solar energy. However, in network some applications need continuous monitoring and air conditioning are directly handled by solar energy.

Sokullu and Demir (2014) study a large group of applications-monitoring of pipelines, roads and bridges as well as recently evolving "Internet of Things" (IoT) applications specifically requires linear topology. In linear topology network, it limits the neighbor nodes and the possible routes so the data delivery is more failure. Linear wireless sensor network with long chain MAC protocol is introduced where the forwarding nodes book in advance and forward packets to reduce end-to-end delay in "long sensor networks" without sacrificing energy efficiency. Performance metrics improved based on the parameters such packet delivery ratio, average end-to-end delay and energy consumption.

Sutagundar and Manvi (2013) study an event triggered multipath routing in WSNs by employing a set of static and mobile agents. Every sensor node is assumed to know the location information of the sink node and itself. This event triggered multipath routing is employed to obtain reliable packet transfer from the source to destination. Initially, the event node fixes the midpoint between the sink and event node. Then, the event node finds the shortest path by the help of location information the nodes above and below the axis is called intermediate nodes. During the transmission, each mobile agent collects the path information and reports it to the sink. By this partial topology multi path is constructed and path weight is also calculated. Now, the sink node selects the path based on the criticalness of an event. If the event is not critical single path is selected otherwise multipath is selected for reliable transaction.

MATERIALS AND METHODS

System model

Network Deployment model: In Fig. 1, sensor nodes are randomly deployed in network using random graph theory. In this architecture, we have N number of sensor nodes and sinks. Each sensor node $n_i \in N$ has assigned a unique Node_ID. The undirected graph G = (V, ε) represents the wireless sensor network where V = {v_1, v_2, ...} represents the nodes and ε = {(v_i, v_j)/v_i, $v_j \in v$} represents the edges. The distance between any two nodes v_i and v_j is denoted as d. A node in the network can either be act as a queen node or drone node. If there exists path between any two nodes v_i and v_j both are within the transmission Range (R) then edge value ε_{ij} is determined by Eq. 1:

$$\varepsilon_{ij} = \begin{cases} 1, \{d(V_i, V_j = E_{Res})\} \leq R \\ 1, \{d(V_i, V_j = 0\} \quad R \end{cases} \tag{1}$$

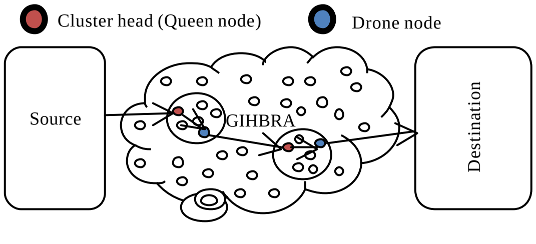

Fig. 1: System architecture

SEE-AMRoute Architecture: Our proposed protocol provides framework for focusing on both network performance and security strength which considering equally important and achieving a good trade-off between two extremes. Consequently, network performance has been measured with metrics of scalability, robustness, reliability and security which becomes an important concern in a resource constrained wireless sensor networks. To boost up the routing process against attacks in routing protocol, framework has the energy efficient routing algorithm along with optimized homomorphism signature for node authentication. This architecture mainly focuses on the following considerations:

- Energy efficiency Analysis has been proposed using various metrics
- Green Indemnity Honey Bee Routing algorithm (GIHBR) has been proposed to establish route and to improve the reliability of the network, threshold based link break detection mechanism has been offered
- Using Optimized Homomorphism Signature algorithm, a collaborative node authentication technique has been offered (Fig. 2)

Working principles of GIHBR algorithm

Protocol description: The GIHBR is an event driven and on-demand multipath routing protocol for wireless sensor networks. GIHBR is mainly focused on cluster formation and Cluster Head (CH) selection, finding the shortest path, multipath construction using honey bee technique and provide security for node authentication. The first phase is to build cluster formation and cluster head selection. The second phase is the route discovery phase in which we have to find the energy efficient shortest path between source node and sink node using honey bee technique and constructing the multiple path for data transmission according to link energy level. This adopts the self-healing mechanism in networks. Whenever link failure occurs, this protocol consider the next route path with second highest link energy level. Last phase focused on security for node authentication.

Node initialization in sensor network: Assume that the whole network has been initialized completely and each node n_i has its own unique Node_ID and its Residual energy level. Such information is called as Initial Node Information (INInfo) message.

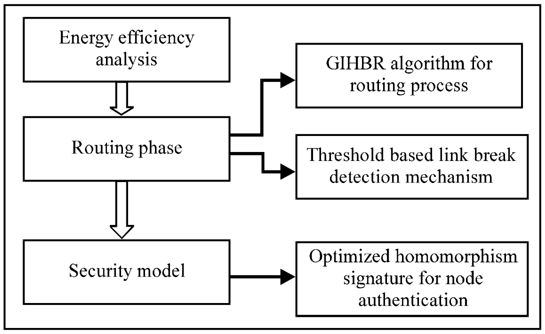
Energy efficiency analysis
Routing phase
Security model
GIHBR algorithm for routing process
Threshold based link break detection mechanism
Optimized homomorphism signature for node authentication

Fig. 2: The SEE-AMRoute architecture

Event_ID	Node_ID	Initial E_{Res}	Event_Time stamp (T)

Fig. 3: The INInfo message packet format

Cluster formation: In WSN, each node has its own Node_ID and Node Residual Energy level Information. Such information is called as Initial Node Information (INInfo) message. Whenever, an event occurs in the network, all the nodes nearby are activated and these are sense its attributes accordingly. Such nodes in this way formed as cluster. Each node can calculate its energy level by using Eq. 2 and it is in the field of E_{Res}:

$$\text{Energy} = \text{Power} \times \text{time} \tag{2}$$

Immediately, they are broadcasting its INInfo Message and its packet format is shown in Fig. 3. Hence, node with highest residual energy will be selected as initial Cluster Head (CH) and this node becomes the Queen node.

Other nodes become the cluster members. Member nodes will forward its sensed data to the initial cluster head (Queen node). Queen node (CH) collects the data and aggregates the data from the member nodes. Besides, QN will execute the route discovery process to find the shortest path. Finally, QN will send the data to the sink node through the shortest path until event stops.

Route discovery phase: Our protocol follows the steps to perform the route discovery process:

Step 1: A node which is selected as queen node in cluster formation phase that has a packet to forward and hence runs the route discovery process using honey bee technique.

Step 2: Neighbour nodes with one hop away from sending node (queen node) are considered as drone bees of the colony.

Step 3: To authenticate all the drone nodes, SEE-AMRoute protocol executes the OHS algorithm. As a result, all the drone nodes are authenticated. To determine the drone node with high energy level, Go to step 4.

Step 4: By using energy fitness function, queen node selects one of drone nodes. Hence Node with highest residual energy is selected as drone node which is included in the route path. Here, fitness function of drone node d_i is calculated with its energy and its distance to the sink node as mentioned in the Eq. 3 (Gudakahriz, 2012):

$$\text{Fitness } d_i = \left(\frac{\text{energy}_i}{\text{max\_energy}}\right) \times \left(\frac{\text{max\_distance}}{\text{distance}_i}\right) \quad (3)$$

Step 5: When one drone node is selected, all the neighbour nodes of this selected drone node are considered as Brood bees of the colony. Now, drone node becomes the queen node and all the brood bees of the colony become the drone nodes.

Step 6: Steps 2-5 are repeated until the en-route path is established between source node and sink node in the network. The en-route path consists of set of queen nodes and drone nodes with highest link energy. At every stage, the selected queen node and drone node information are recorded in the routing table which gives the overall route path information.

Route is discovered based on above mentioned process and route information is recorded in all intermediate queen nodes and drone nodes along the route in the form of route table entries. Since, queen nodes do not have any route information, the route discovery process can be initiated by each queen node by sending a drone packet. To discover the drone node, queen node will broadcast a DReq packet to its neighboring nodes. Here, we have considered neighbors with one hop count. This assumption will reduce the excess communication overhead to route discovery process. Since, TTL value is 1, DReq Packet will never further be forwarded to next hopping process. After a packet has been broadcasted, a QN will wait for DReply packet. DReq packet and DReply packet Fformat information is shown below (Fig. 4 and 5).

Event_ID	QN_ID	Source_ID	Dest_ID	TIL

Fig. 4: The DReq packet format

Event_ID	DN_ID	DN_Eres	Hop_Count	Node status

Fig. 5: The DReply packet format

Event_ID	Source_ID	Dest_ID	QN_ID	QN_Eres	Next_Hop		Link energy
					DN_ID	DN_Eres	

Fig. 6: Routing table

Event_ID	DN_ID	DN_Eres	Node status

Fig. 7: Drone table

As soon as QN receives DReply packet, QN will collectively keep all the DReply information into a one table known as drone table which contains drone nodes information that is neighborhood information.

In drone table, QN will check the node status field. Node status field will maintain status information about the nodes whether node is marked as "selected" or "unselected" to include in the en-route path. Drone node that has already been selected for en-route path, its node status is selected otherwise it is unselected. By using this node status, we can avoid the loop formation in the route discovery phase. However, QN will check the DN_ID in drone table with Dest_ID in routing table. If both are same then QN will arrive at sink node otherwise QN checks the node status field in drone table. If node status is unselected and both DN_ID and Dest_ID are different, then QN selects the drone node based on its energy level. By fitness function Eq. 3, the node with high energy is selected by the cluster head (queen node) is considered as drone node from the cluster. For transmitting data by analyzing the energy of node ensures the reliable data delivery. Once the drone node is selected then it will act as queen node.

After selected the drone node, QN update its routing table entries of next hop field and link energy. Link energy field will give the overall link energy cost for data transmission. The QN field will give the shortest route path to transmit the data. Each node will maintain routing table containing information shown below in Fig. 6 and 7. Thus, above routing process will be

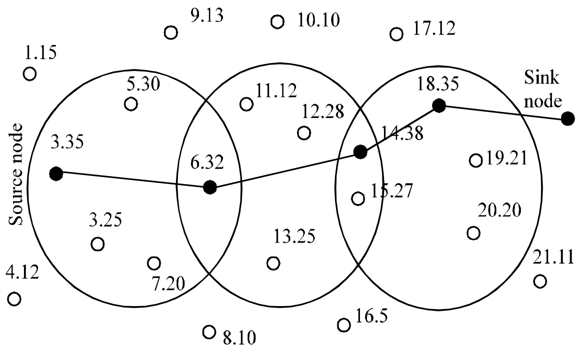

Fig. 8: Network structure

explained by considering an example of 22 nodes and finding a path from a source node to a sink node as shown in Fig. 8.

In Fig. 8 node 2 is a source node with energy cost of 35 that has the data to forward to sink node. This node will select the drone node 6 with highest energy cost 32 which becomes the queen node. Likewise, we will find out the collection of queen nodes and drone nodes which give shortest route with high energy for transmission. We have route path root1: n2→n6→n14→n18→sink node and its total link energy cost is 140 exclude with sink node energy. Besides, root2: n2→n5→n12→n15→n19→sink node and its total link energy are 141. Here, total link energy cost is the sum of the energy of all transmitting nodes in route path.

Route maintenance phase: Once the route is established then the process of route maintenance plays an important role in routing protocols. Route maintenance is required to repair the broken links. Due to the dynamic nature of sensor nodes, the links between nodes break down frequently. Unavailability of any node in between source node and destination node may lead to a link break. This occurs either when a node goes beyond the transmission ranges of its neighbor or when the energy level of a node is not sufficient to send or receive a packet. Every node in active path consumes a certain amount of energy for the active participation in communication. As, the energy level goes down and reaches a minimum the associated link becomes unavailable. Limitation on transmission range and mobility can also be the reason for link failure. Alternate route discovery in AMRoute suffers from end to end delay and data loss as the routing table stores only one route to a destination.

Threshold based link break detection mechanism: Whenever link break is detected, this protocol will select next available route path for data transmission. By using drone table, we can obtain the second highest energy route path which is mainly used to update the routing table information. Suppose, no route path is available to sink node then route discovery process is initiated by this phase. Alternate route path can be selected quickly by using drone table without delay and data loss incurred by link break. Maintaining of multiple route path information in routing table introduce the self healing mechanism in network. As a result, our proposed protocol enriches the performance of reliable data transmission.

Generally, link breaks are detected either in route discovery process or during the data transmission. Since, sensor node has known about the transmission Range (R), queen node calculates the expected arrival time of DReply packet. Here, this expected arrival time is considered as the threshold value whose formula:

$$\text{Thi} = \sum_{i=1}^{n} \text{EADRi}$$

where, EADR_i is the expected arrival time of Dreply packet. During the data transmission, the Ti should be lies between the value of $\text{di} \leq \text{Th}_i \leq \text{md}_i$. If the Th_i does not satisfy this condition, this may cause the line breaks.

Data transmission: Queen node calculates the total size of the information to forward and its total energy required for transmission which is shown below. The energy consumption is calculated by the product of total amount of power consumed and time required for the whole transaction:

$$\text{Pt} = \frac{8 \times \text{packet size}}{\text{Bandwidth}} \quad (5)$$

The transmitting energy $E_{tx}$is measured as:

$$E_{tx} = P_{tx} \times P_t \quad (6)$$

The receiving energy $E_{rx}$is measured as:

$$E_{rx} = P_{rx} \times P_t \quad (7)$$

Energy consumption of a node after time t is calculated using Eq. 8:

$$E_{con(t)} = N_t \times C_1 + N_r \times C_2 \quad (8)$$

Where:

Econ(t) = The energy consumed by a node after time (t)
N_t = Number of packets transmitted by the node after time (t)
N_r = Number of packets received by the node after time (t)
C_1 and C_2 = Constant factors having a value between 0 and 1

The CH perform step 3, 4 again until packet delivery is successful. Let E be the initial energy of a node and the residual energy E_{res} of a node at time t can be calculated by using Eq. 9:

$$E_{Res} = E - E_{con(t)} \tag{9}$$

Where:

E_{res} = Residual energy
E_{con} = Consumed energy

That is, total energy consumption of all Nodes is measured as the summation of all node's residual energy plus the product of initial energy and number of nodes.

$$TE_{con} = N \times \text{Initial energy} - E_{Res} \tag{10}$$

Where:

TE_{con} = Total consumed energy
N = Total number of mobile nodes in the network

If the selected route path energy is higher than the forward data energy then this route path is considered for routing. Otherwise, if selected route path energy is not sufficient to forward data, this protocol will consider selected route path as path_1 and choose the next available route path with higher link energy for transmission as path_2 from drone table. Hence, protocol will forward the data by using various route path such as Path_1 and Path_2. As a result, protocol can able to forward data through multi path. Hence, proposed protocol achieved the maximum throughput without packet loss. Besides enhance the lifetime of the network and utilized the scared bandwidth very efficiently.

Security model: By combining honey bee techniques with Optimized Homomorphism Signature algorithm, this framework derives a dynamic model that efficiently describes routing mechanisms under attacks. As a result, we develop a protocol which ensures secured network connectivity and stability against attacks.

Kanawat and Parihar (2011) stated that an attacker physically captures nodes and compromises them such that readings sensed by compromised nodes are manipulated or inaccurate. In addition, the attacker may attempt to extract essential cryptographic keys (e.g., a group key) from wireless nodes that are used to protect communications in the very most wireless networks.

Optimized homomorphism signature: Whenever, route discovery process is initiated by the node, node executes the Optimized Homomorphism Signature algorithm for node authentication.

Key generation process:

```
Key_Generation
{
   Choose two large prime numbers p and q in Z*.
   Compute Public Key PK = p*q.
    Choose a secret number S between 1 and n-1.            Keeps S as
Private Key.
   Return (PK,S)
}
```

OHS procedure:

```
Input:  Number of Sensor Nodes
Begin
While QN sending DReq Packet, QN computes
     $MAC_{Sou}$  _  $Enecrypt_S$ [ h($MAC\_ID_q$ +SK) || $R_s$ ]
  QN send DReq Packet along with $MAC_{Sou}$ value for Node
   Authentication.
 //   Assume that, $n_1$,$n_2$,$n_3$ …. $n_i$ denotes the number of drone nodes
On receiving DReq packet, Drone node proceeds
For each drone node $n_i$  do
    Begin
         Get $MAC\_ID_{qi}$  of source node from MAC_TABLE.
         $MAC_i$ = $Decrypt_{PK}$ [   $MAC_{Sou}$   ]
         New $MAC_i$ = h( $MAC\_ID_{qi}$ +SK)
         Compare if new $MAC_i$  = = $MAC_i$ then
          Send DReply Packet with $R_s$ value by $n_i$
          Else  Set M_ID = QN_ID
               //which is broadcast to neighborhood
   Endfor
On receiving DReply packet, Queen Node proceeds Verify $R_s$ value with the
received $R_s$, proceed if all correct. Otherwise,
         Display " Malicious Node "
         Set M_ID = DN_ID
            //which is broadcast to neighborhood
 End
```

OHS algorithm determines the collection of trusted nodes in the network which are collectively form the secure link (path) for data transmission. Hence OHS provides link security.

RESULTS AND DISCUSSION

Energy analysis: By observing the energy consumption of existing protocols, the analysis is done in by considering different parameters that are included during the transmission such as time, distance, routing method, storage and congestion. By analyzing the LEACH, EEICCP (Energy Efficient Inter Cluster Coordination

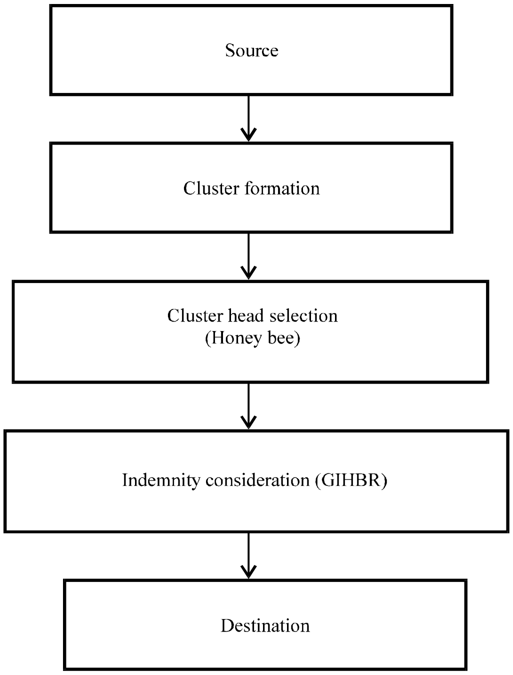

Fig. 9: Workflow of proposed system

Protocol) and DEEP (Deterministic Energy Efficient Protocol) are considered to analyze the energy consumption based on the above mentioned parameters. Our proposed GIHBR is analyzed based on the parameters mentioned above, the time consumption is less due to the shortest path selection for the transaction, even though the shortest path is selected, proposed algorithm canvas the maximum distance, the efficiency of routing process is calculated by ensuring the reliability in the transaction by assuring the alternate path, storage capacity is enhanced by removing the duplicates in the storage using data aggregation automatically improves the processing time and finally by assuring the reliable delivery it reduces the traffic occurrence leads to reduction in congestion.

The following analysis shows that the proposed GIHBR is compared with the few existing protocol and the result process are shown as below. It is compared with the parameters like throughput, packet delivery ratio and energy consumption (Fig. 9).

Figure 10 shows the comparison between the above mentioned protocols, it shows that the proposed algorithm throughput value is high. Figure 11 shows the comparison between the above mentioned protocols, it shows that the proposed algorithm obtain high packet delivery ratio. Figure 12 shows the comparison between the above mentioned protocols, it shows that the proposed algorithm obtain less energy consumption.

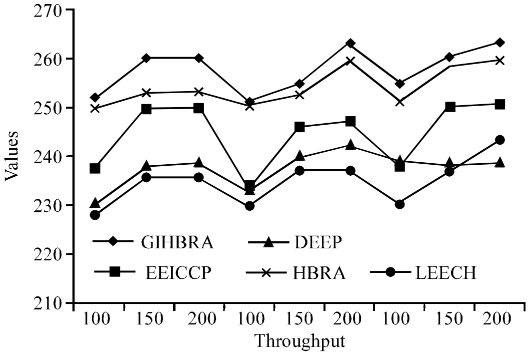

Fig. 10: Performance evaluation by throughout

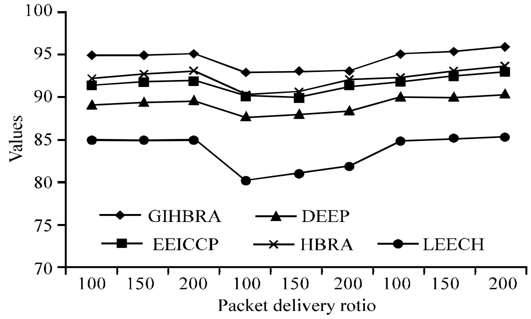

Fig. 11: Performance evaluation by packet delivery ratio

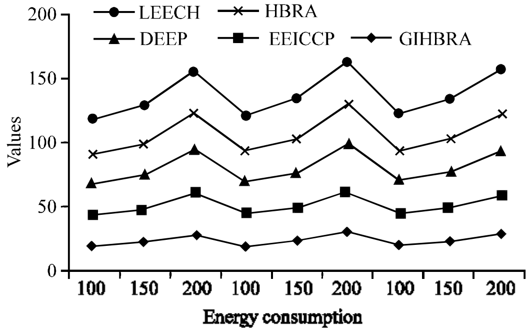

Fig. 12: Performance analysis by energy consumption

Performance analysis: We have simulated our results using NS2.34 simulator. It is an object oriented discrete event simulator to identify the performance of proposed scheme. The Backend language of NS2.34 is C++ and front end is Tool command language (Tcl). The NS2 is user friendly and easy to fabricate our own protocol. Tcl is a string-based command language. The language has only a few fundamental constructs and relatively little syntax, which makes it easy to learn. The syntax is meant to be simple. Tcl is designed to be glue that assembles software building blocks into applications. Here, we made the assumption that adopted for simulation is all nodes are moving dynamically including the direction and speed of nodes.

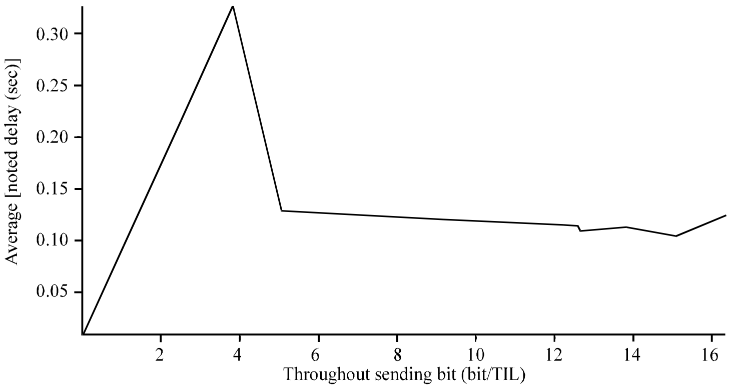

Fig. 13: Average end to end delay of sending bytes; send event time vs simlation End2End delay X: send event time STL: AGT DTL: AGT

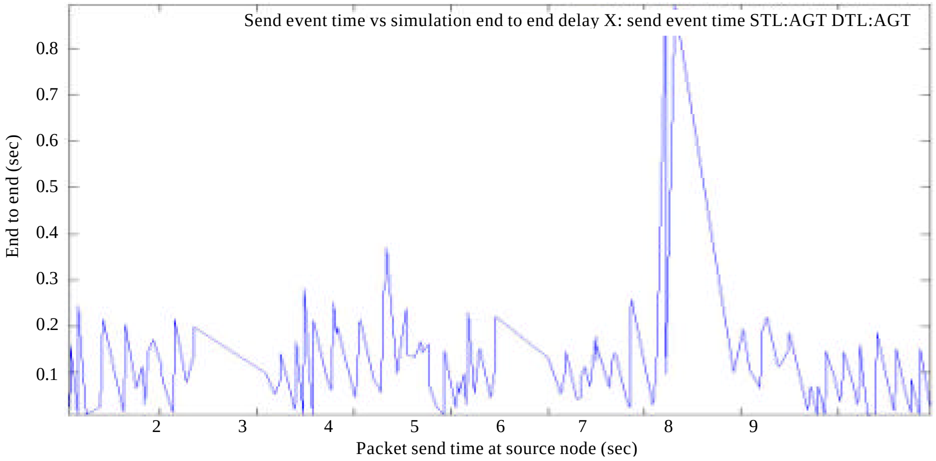

Fig. 14: End to end delay of source node

In our simulation, 100 mobile nodes move in a 1200×768 region for 300 sec simulation time. Our simulation settings and parameters are summarized in Table 1-3.

Performance metrics: We evaluate mainly the performance according to the following metrics.

End-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Packet delivery ratio: It is defined as the ratio of packet received with respect to the packet sent.

Throughput: It is defined as the number of packets received at a particular point of time.

Communication overhead: The communication overhead is defined as the total number of routing control packets normalized by the total number of received data packets.

Table 1: Simulation settings and parameters of proposed scheme

Parameters	Values
No. of nodes	100
Area size	1200×768
Simulation time	300 sec
Traffic source	CBR
Packet size	15000 bytes
Protocol	GIHBR

Energy consumption: Minimum energy is maintained among all the Queen nodes in the network.

Network lifetime: It defines how long the sensor nodes live with more residual energy. The simulation results are presented.

In Fig. 13, end to end delay of sending bytes average result is shown with respect to the throughput in the graph. Our proposed scheme GIHBR achieves better end to end delay of sending bytes.

In Fig. 14, end to end delay of packet send time at source node in seconds is shown in the graph. Our proposed scheme GIHBR achieves better end to end delay of source node.

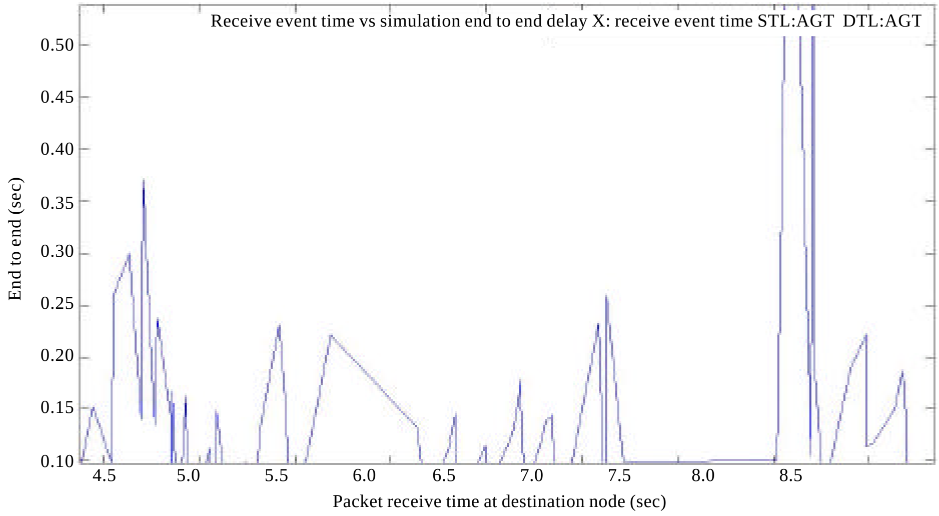

Fig. 15: End to end delay of destination node

Table 2: Analysis of proposed methods in terms of different parameters

Metrics	GIHBR
Energy consumption (Joules)	19.48 J
Delivery ratio (%)	89%
End to end delay (m sec)	160 m sec
Communication overhead (pkts)	235-294

Table 3: Energy model

Parameters	Value
Initial	100 Joules
T*Power	2.0 J
R*Power	1.5 J
Sleep power	0.05 W
Idle power	0.5 W

In Fig. 15, end to end delay of packet receiving time at destination node in seconds is shown in graph. Our proposed scheme GIHBR achieves better end to end delay at destination side.

CONCLUSION

In WSNs, sensor nodes are arranged randomly due to the movability of nodes in the network. Packet transaction, security, energy consumption and effects of rays living beings are the issues. Here, we focus on to minimize energy consumption and increasing the network lifetime of the network. So, we propose GIHBR Algorithm which involves honey bee approach to forward the packet from source to destination in less energy consumption by including the indemnity of the network in a secure manner. All these technique is implemented in green wireless sensor network which avoids affects to living beings. By using NS2, a discrete event simulator, our scheme achieves secure transaction with less energy consumption, delivery ratio, reduced overhead, low end to end delay and throughput.

REFERENCES

Aweya, J., 2013. Technique for differential timing transfer over packet networks. Ind. Inf. IEEE. Trans., 9: 325-336.

Chen, Q., S.S. Kanhere and M. Hassan, 2009. Analysis of per-node traffic load in multi-hop wireless sensor networks. Wirel. Commun. IEEE. Trans., 8: 958-967.

Cheng, C.T., C.K. Tse and F.C.M. Lau, 2011. A clustering algorithm for wireless sensor networks based on social insect colonies. IEEE Sens. J., 11: 711-721.

Gudakahriz, S.J., S. Jamali and M.V. Khiavi, 2012. Energy efficient routing in mobile ad hoc networks by using honey bee mating optimization. J. Adv. Comput. Res., 3: 77-87.

Kanawat, S.D. and P.S. Parihar, 2011. Attacks in wireless networks. Int. J. Smart Sens. Ad Hoc Netw., 1: 113-116.

Poonguzhali, J.K.B.P., 2014. Energy balanced routing method for in-network data aggregation in wireless sensor networks. IOSR. J. Electron. Commun. Eng., 9: 05-14.

Sahoo, R.R., M. Singh, B.M. Sahoo, K. Majumder and S. Ray *et al*., 2013. A light weight trust based secure and energy efficient clustering in wireless sensor network: Honey bee mating intelligence approach. Proc. Technol., 10: 515-523.

Sokullu, R. and E. Demir, 2014. Investigating energy efficiency and timeliness for linear wireless sensor networks. Proc. Comput. Sci., 37: 24-31.

Sutagundar, A.V. and S.S. Manvi, 2013. Location aware event driven multipath routing in wireless sensor networks: Agent based approach. Egyptian Inf. J., 14: 55-65.

Thayananthan, V. and A. Alzranhi, 2014. Enhancement of energy conservation technologies in wireless sensor network. Proc. Comput. Sci., 34: 79-86.

Yuea, J., W. Zhang, W. Xiao, D. Tang and J. Tang, 2012. Energy efficient and balanced cluster-based data aggregation algorithm for wireless sensor networks. Proc. Eng., 29: 2009-2015.

Zhang, H.B. and H. Shen, 2010. Energy-efficient beaconless geographic routing in wireless sensor networks. IEEE Trans. Parallel Distrib. Syst., 21: 881-896.