Cluster based Energy-Efficient and Reliable Routing for Mobile Wireless Sensor Networks

Mr. Amol Deshmukh
M.E Student,Department of Computer Science
G.H. Raisoni Institute of Engineering and Management
Jalgaon,India
amol2050@gmail.com

Mr. Rahul Chinchore
Asst. Professor, Department of Computer Science
G.H. Raisoni Institute of Engineering and Management
Jalgaon,India.
Rahul.chinchore@gmail.com

Abstract—The main problem of energy efficient reliable routing is that it doesn't provide any back up mechanism for the failure of the nodes. The work of the paper major depends on the alternate path provided if the link got failure and to provide energy efficient path in between the network.it will reduce the time,cost and increase the efficiency and the data rate of the network.
In wireless sensor networks, because of unreliable wireless media, host mobility and lack of infrastructure, providing secure communications is bit difficult in this type of network environment. In present work to ensure the security in unreliable wireless communication the cluster based topology technique is used, to obtain confidentiality and authentication of nodes hash function and MAC (Message Authentication Code) techniques are used

*****

I. INTRODUCTION

A.Wireless sensors Network

A wireless sensor network (WSN) of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc. and to forward their data through the nodes in network to a main server.

The Implementation of WSN was motivated by military applications, they are used for battlefield surveillance. Now a days WSN networks are used for consumer and industrial applications, also in industrial monitoring and control of the process, monitoring of machine health.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Every sensor node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node size might vary from that of a shoebox down to the size of a grain of dust.. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of rupees, which depends on the complexity of the every individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding resources constrains such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can differ from a simple star network to an advanced multi-hop wireless network. The navigation technique between the hops of the network can be flooding or routing.

The main characteristics of a WSN include:

- Power consumption parameter for nodes using batteries or energy harvesting
- Ability to handle with node failures
- Mobility of nodes
- diversification of nodes
- Scalability to very large scale of deployment
- Ability to handle harsh environmental conditions
- Ease of use
- Cross-layer design

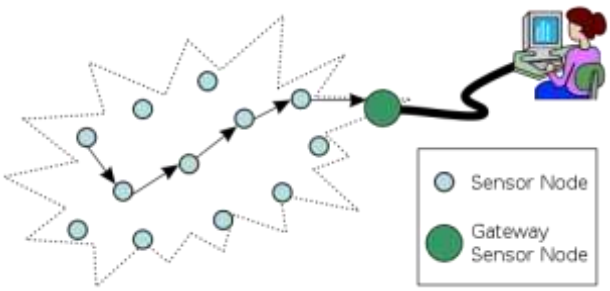


Figure 1.1: Typical Multihop Wireless Sensor Network

II. PROBLEM DEFINITION

The multihop routing in wireless sensor networks (WSNs) offers little protection against identity deception through replaying routing information. An adversary can exploit this defect to launch various harmful or even devastating attacks against the routing protocols, including sinkhole attacks, wormhole attacks, and Sybil attacks.

However the most prominent works in the related fields has been done by Guoxing Zhan, Weisong Shi, et Al i.e. "Design and Implementation of E2R2 : A Trust-Aware

Routing Framework for WSNs". Without tight time synchronization or known geographic information, E2R2 provides trustworthy and energy-efficient route. Most importantly, E2R2 proves effective against those harmful attacks developed out of identity deception; the resilience of E2R2 is verified through extensive evaluation with both simulation and emperical experiments on large-scale WSNs under various scenarios including mobile and RF-shielding network conditions[18].

In E2R2 neighborhood table is generate for route selection where values are same in respect to all nodes. How it can be efficient or most accurate routing of packets? this results into increasing end to end delay. So efficient routing is necessary while implementing framework.

E2R2 also ignoring any packet level security and it becomes necessary to find appropriate protection as the data may include some sensitive information which should not be accessed by or can only be partially exposed to the general users. So in the recent world, security is a prime important issue, and encryption is one of the best alternative ways to ensure security. So while packet security should consider in implementation of framework.

E2R2 needs high packet delivery rate. But link failure situation is not taking into consideration. When packet comes to the node for forwarding, it decides path by using trust manager and neighborhood table. And if link failure occurs due to some reason after selecting path for routing then packet loss is occurs. Due to this packet loss rate is increases and packet delivery rate decreases.

This is all about E2R2 , which is existing system for trust aware routing and preventing identity deception attacks.

Now for link failure resiliency, Srinivasan Ramasubramanian proposed "Dual-Link Failure Resiliency through Backup Link Mutual Exclusion" which classifies the approaches to dual-link failure resiliency. BLME- Backup Link Mutual Exclusion is good methodology for link failure recovery[16].

BLME algorithm generates backup paths extra before routing packets. If some link fails then that already generated backup path is used. And in this way link failure is recover. But if deeply observe backup path generation of BLME then it can be note that BLME algorithm generates much of alternate paths at time before from source to destination without need to any link failure occur. So in case when link failure does not occurs then these generated paths are waste in terms of generation time, computation cost as well as it increases delay to packet reach at destination. And in other case if link failure occurs then also numbers of other paths are waste. Which affect delay time and computation cost.

Proposed system "Robust framework for preventing identity deception attacks using backup path generation" is system which follows Trust aware routing of E2R2 and improved by including packet security, efficient routing technique for increasing packet delivery rate. Integrated with BLME methodology of backup path generation for link failure recovery for decreasing packet loss rate and End to End Delay and increasing packet delivery rate which is also improve with efficient backup path generation for low computation cost and minimum delay.

Goals & Objective of E2R2

E2R2 mainly guards a WSN against the attacks directing the multi-hop routing, especially those based on theft through replaying the routing information. This system does not address the denial-of-service (DoS) attacks, where an attacker intends to affect the network by using its resource. For instance, we do not address the DoS attack of congestion network by resending numerous packets or physically blocking the network. E2R2 aims to achieve the following desirable properties: High Packet delivery rate, Energy Efficiency, scalability and adaptability.

However, link failure condition is also taking into consideration by E2R2 . So, packet loss, time delay such things happen due to link failure should be consider when we want to achieve high throughput[1].

III. PROPOSED PROTOCOL

In the proposed a novel energy-aware routing algorithm, called reliable minimum energy cost routing (RMECR). RMECR finds energy efficient and reliable routes that increase the operational lifetime of the network. RMECR is proposed for networks with hop-by-hop (HBH) retransmissions providing link layer reliability, and networks with E2E retransmissions providing E2E reliability. It considers the energy consumption and the remaining battery energy of nodes as well as quality of links to find energy efficient and reliable routes that increase the operational lifetime of the network[3].

Proposed Algorithm

A.Classifications of the sensor nodes

In this paper, we divide the specially-functional sensor nodes into three categories:

BN (Branch Node): BNs are the one-hop neighbors of the BS. Each BN represents one branch. The nearer to the BS, the node has more burdens on data transmission. The BN acts critical role in the network, because once it's exhausted the whole branch is separated and the downstream paths are correspondingly failed. In order to conserve energy, the BN doesn't join the cluster formation and data sense. It just acts as a router in the network.

Furthermore, if its energy is below a limitation value, it should announce that it abandons the role of branch node and transforms to a normal node.

CH (Cluster Head): In our approach, cluster heads are elected distributed based on the parameters of the residual energy and the number of neighbors. CH is in charge of data receive, data process, data aggregation and data transmission. The energy consumption of CH is much quickly than normal nodes.

SN (Substitute Node): The substitute nodes for CHs. This strategy guarantees the data could be transmitted correctly even if the cluster head is exhausted. This could improve the reliability and fault tolerance of the system. The remained nodes are normal nodes.

Process of EERRP

The operation of EERRP is divided into different rounds. The BS periodically collects the sensed data and initializes a new round by sending a request message. In every round, EERRP runs the following three phases:

Phase one: Broadcast

This phase starts from the BS broadcasting a request message. The format of this message is {REQ, RID, BID, SID, Ere, HCount, Eto, N}, where REQ indicates the type of message is request; RID is the round identifier, which is generated by the base station; BID is the identifier of the branch, i.e., identifier of the branch node; SID is the identifier of the sender node; Ere is the residual energy of the sender node; HCount is the hop counts from the sender to the base station; Eto indicts the total energy of all nodes, it's calculated by the base station; Finally N is the sum of nodes after last round. Here Eto and N are prepared for the election of cluster heads. The BS initially broadcasts the message {REQ, RID, F, BS, ∞, 0, Eto, N}.

After this phase, every node decides whether it is a Branch Node, stores the parameters (Eto, N) for the next phase, and records the neighborhood information, which provides a primary path and a few alternative paths to the

BS. Each node rebroadcasts once and only once.

Phase Two: Cluster Formation

After previous phase, every node has the information about the total energy Eto and sum of nodes N. Each node decides whether to be a cluster head.

Once the node has elected itself to be cluster head, it broadcasts an advertisement message (ADV) using a non-persistent carrier-sense multipath access (CSMA) MAC protocol . Each non-cluster head node determines its cluster for this round by choosing the cluster head that requires the minimum communication energy, based on the received signal strength of the advertisement from each cluster head.

After each node has decided to which cluster it belongs, it transmits a join-request message (Join-REQ) back to the chosen cluster head using a CSMA MAC protocol.

The cluster head node sets up a TDMA schedule and transmits this schedule to the nodes in the cluster.

Besides, in order to improve the fault tolerance of the cluster, CH need elect one node as the substitute of the cluster head. CH will choose it from the nodes whose Join-REQ messages are heard by CH with the larger signal strength, i.e., they are closer to CH than others.

Then CH compares the energy and neighbor number amongthese node, finally elects one node with higher parameters. CH sends a announcement message (SNANN) to nodes. This message consists of the SNANN header, the node's ID and the CH's ID. The ID matched node marks itself as a Substitute Node after hearing the message.

Phase Three: Data Propagation

This phase consists of two steps: first the data propagation within a cluster, then the data propagation from the cluster head to the BS, which is along multi-hops.

In a cluster, nodes send their data to the cluster head during their allocated transmission slot time. Once the cluster head receives all the data, it performs data aggregation to enhance the common signal and reduce the uncorrelated noise among the signals. In our approach, after every round, BS needs to know the whole residual energy of all nodes and the sum of nodes alive.

During this process, if the residual energy of the cluster head is below a limitation value Eurgent, it will broadcast an energy-urgent announcement message, and send the received data to the substitute node. The remaining nodes which haven't yet sent data change the cluster head correspondingly. It's a very reliable and flexible fault tolerant scheme.

Then the resultant data are sent from the cluster head tothe BS. Since the BS may be far away and the data messages are large, this is a multi-hop and high-energy transmission. The cluster head firstly checks its neighborhood. The node marked with "parent" is the next hop and the path is the primary path along it. Then CH continuously looks for the neighbors with different BID value from its parent. After comparing the energy and number of neighbors, the CH chooses the next hop nodes (more than one).

After the next hop nodes are chosen, the CH (intermediate node) transmits data along the primary path at first. If the data is successfully sent to the next hop, the next hop will response a SUCCEED message. After a certain threshold time, if CH didn't get the response message, it will send the data along another next hop.

The message sent from CH includes message type (DATA), next hop ID, BID, aggregated data, Ncluster and Ecluster. For inter-media nodes, it checks the BID, finds next hop with the same BID in its neighbors and transmits data to it. Similar to last step, it waits SUCCEED message from the next hop for a certain threshold time. If it can't get the response message, it will send a FAILURE message back to its last hop. If any inter-media node receives the FAILURE message, it will notice its last hop till CH gets the information.

Algorithm 1

1. Initially BS collects information regarding of all the nodes in the network.

(a) BS transmit message to all nodes in the network

2. Assigning energy to all nodes.

3. Choose the source and destination.

4. To find the neighbours.

(a) First find HBH transmission

(b) If this route is reliable then E2E route is reliable

5. Choose the shortest routing using Dijkstra's algorithm

(a) Dijkstra's algorithm is only heuristic solution for find minimum energy cost path.

(b) C(P(s,v))=C(P(s,v))+W(u,v)

6. Calculating the minimum energy routing path for usingMinMax algorithm

7. Sending packets through the reliable path.

Security in key Distribution

Here considers a cluster-based ad hoc hierarchical network topology. A subset of the network nodes is selected to serve as the network backbone over which essential network control functions are supported. The approach to topology control is often called clustering, and consists of selecting a set of cluster heads in a way that every node is associated with a c1uster head, and c1usterheads are connected with one another directly or by means of gateways ,so that the union of gateways and c1usterheads constitute a connected backbone. Once elected, the cluster heads and the gateways help reduce the complexity of maintaining topology information, and can simplify such essential functions as routing, bandwidth allocation, channel access, power control or virtual-circuit support.

The basic steps for attaining the comparative analysis are given below.

A. Turn on Tracing Window

This window traces the simulation events at each and every seconds of the given simulation period.

B. Turn on Tracing Window

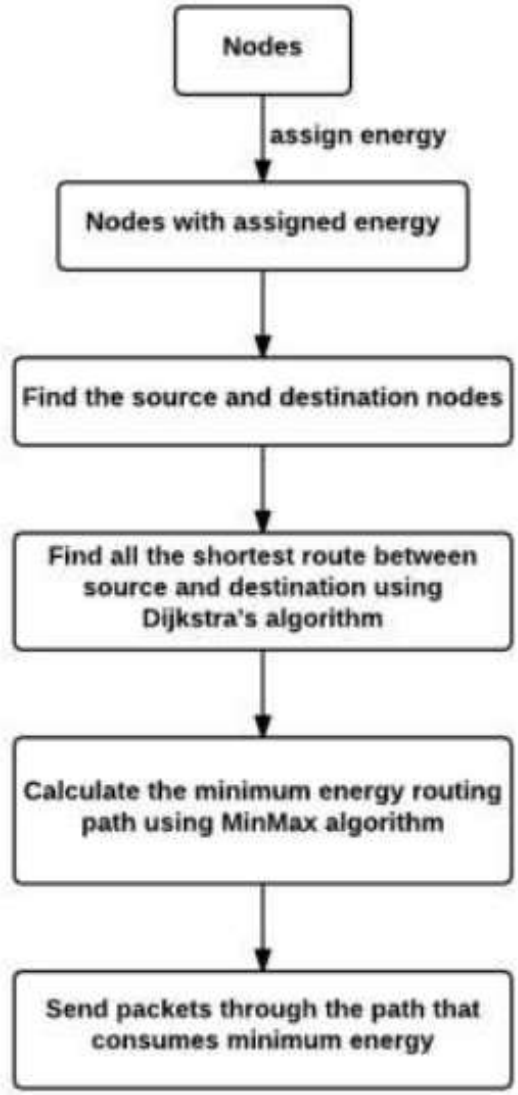
The next step is to give topology for the network. For the WANET, the specified topology is MESH. For any wireless network, it is necessary to give all the necessary parameters like type of channel, type of ad-hoc routing protocol, type of antenna, etc.

C. Turn on Tracing Window

This section will create the appropriate routing agents forthe data flow. In WANET, TCP has been used. It is much more reliable than the other and it is the one which has been supported easily by NS-2.It provides the routing algorithm for the network.

D. Turn on Tracing Window

The script might create some output on stdout, it might write a trace file or it might start name to visualize the simulation. It is a discrete event simulator and very much useful for analysis of dynamic nature of communication network. [4]. The pictorial representation of algorithm shown in Fig.1



 ISSN: 2321-8169
1275 – 1280

Algorithm 2: Cluster formation and leader election

```
1  Input: S // Set of nodes that detected the event
2  Output: u // A node of the set S is elected leader of
       the group
3  foreach u ∈ S do
4      role_u ← coordinator;
       // Node u sends message MCC in broadcast
5      Announcement of event detection ;
       // N_u is the set of neighbors of node u ∈ S
6      foreach w ∈ N_u do
7          if HopToTree(u) > HopToTree(w) then
8              role_u ← collaborator ;
9              Node u retransmits the MCC message received
               from node w ;
10         end
11         else if HopToTree(u) = HopToTree(w) ∧
           ID(u) > ID(w) then
12             role_u ← collaborator ;
13             Node u retransmits the MCC message received
               from node w;
14         end
15         else
16             Node u discards the MCC message received from
               w;
17         end
18     end
19 end
```

Algorithm 3: Route establishment

```
1  Leader node v of the new event sends a message REM to its
   NextHop_v ;
2  repeat
       // u is the node that received the REM message,
          that was sent by node v
3      if u = Nextop_v then
4          HopToTree_u ← 0 ;
           // Node u is part of the new route built
5          Role_u ← Relay ;
6          Node u sends the message REM to its NextHop_u ;
7          Node u broadcasts the message HCM with the value of
           HopToTree = 1;
8          Nodes that receive the HCM message sent by node u,
           will run the command Line 2 until the Line 14 of
           Algorithm 1;
9      end
10 until Find out the sink node or a node belonging to the routing
   structure already established.;
11 repeat
       // sons_u is the number of descendants of u
12     if sons_u > 1 then
13         Aggregates all data and sends it to the nexthop_u;
14         if Role_u = Relay then
15             Execute the mechanism of Section 3.4
16         end
17     end
18     else
19         Send data to nexthop_u;
20         if Role_u = Relay then
21             Execute the mechanism of Section 3.4
22         end
23     end
24 until The node has data to transmit/retransmit;
```

IV. RESULTS

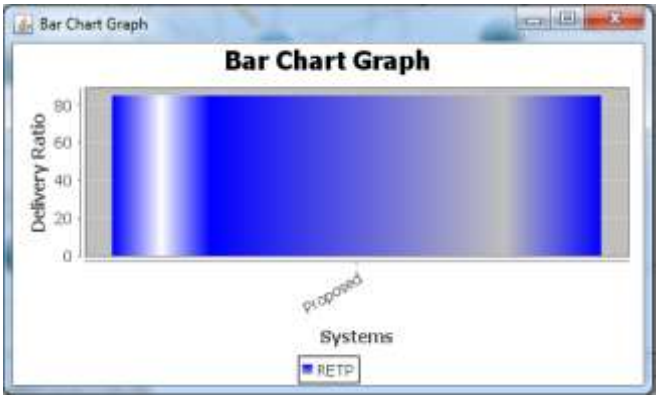


Fig.Delivery Ratio

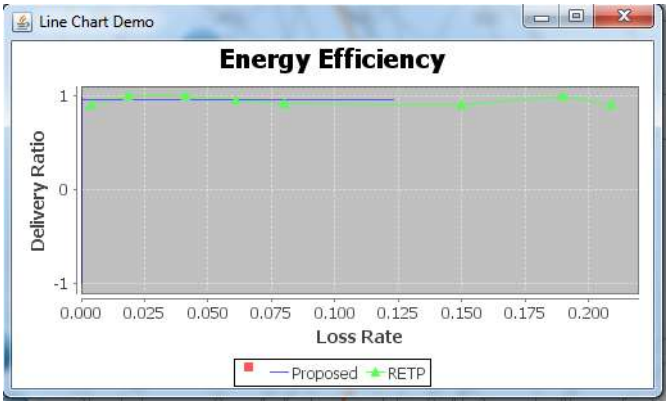


Fig. Energy Efficiency

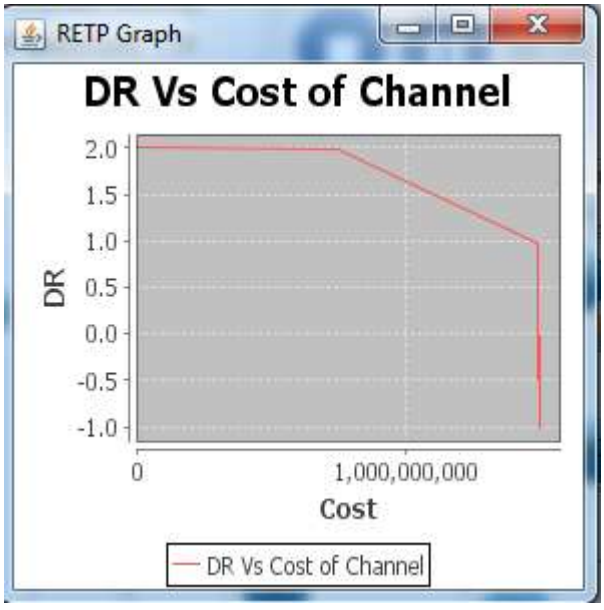


Fig. Data Rate vs Cost

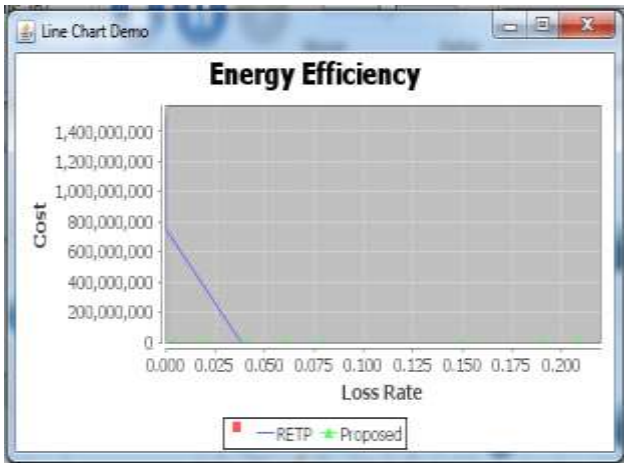


Fig. Cost vs Loss Rate

V. CONCLUSION

In this paper, we have implemented an energy-efficient and reliable routing protocol for mobile WSNs. The proposed protocol E2R2 is hybrid cluster based.

This protocol provides energy efficient routing in between the network,it also provide the backup path if the node got failure while sending information from one node to another.it also provide the security for the data which is going to be send.by choosing the alternate path while the node got failure energy efficient and reliable path will be selected..

The proposed protocol has also been tested under the influence of highly mobile sensor nodes and according to results we can conclude that the proposed algorithm have high throughput even in high data rate, high mobility and in addition it provides high security to data. In future it would be interested to implement proposed algorithm in real world scenario.

VI.REFERENCES

[1] G.Kalpana, Dr.T.Bhuvaneswari, "A Survey on Energy Efficient Routing Protocols for Wireless Sensor Networks", 2nd National Conference on Information and Communication Technology (NCICT) 2011.

[2] Mohammad Masdari1 and Maryam Tanabi2, "Multipath Routing protocols in Wireless Sensor Networks: A Survey and Analysis", International Journal of Future Generation Communication and Networking Vol.6, No.6 (2013), pp.181-192.

[3] K. Vinoth Kumar1, S.Karthikeyan2, " Multihop Energy Efficient Reliable and Fault TolerantRouting Protocol for Wireless Sensor Networks", ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 2, February 2013.

[4] Ning Sun, Young-bok Cho, Sang-ho Lee, "A Distributed Energy Efficient and Reliable Routing Protocol for Wireless Sensor Networks", IEEE International Conference on Computational Science and Engineering IEEE International Conference on Computational Science and Engineering CSE/I-SPAN 2011.

[5] Ali Norouzi1, Faezeh Sadat Babamir2, Abdul Halim Zaim3, "A Novel Energy Efficient Routing Protocol in Wireless Sensor Networks", IEEE 2011.

[6] Satvir Singh, Meenaxi, "A Survey on Energy Efficient Routing in Wireless Sensor Networks", IEEE Volume 3, Issue 7, July 2013.

[7] Monica R Mundada1, Savan Kiran1 ,Shivanand Khobanna1, Raja Nahusha Varsha1 and Seira Ann George1, "A STUDY ON ENERGY EFFICIENT ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORKS", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.3, May 2012.

[8] Ahmed Ali Saihood, Rakesh Kumar, "Enhanced Location Based Energy-Efficient Reliable Routing Protocol for Wireless Sensor Networks", International Journal of Inventive Engineering and Sciences (IJIES) ISSN: 2319–9598, Volume-1, Issue-6, May 2013.

[9] Neha Rathi1, Jyoti Saraswat2 and ParthaPratim Bhattacharya3 , "A REVIEW ON ROUTING