Research Article **ISSN: 2395 – 5597**

International Journal of Engineering and Robot Technology

Journal home page: www.ijerobot.com

ENERGY RESOURCEFUL AND CONSISTENT CLUSTERED ROUTING FOR MOBILE WIRELESS SENSOR NETWORKS

D. Giji Kiruba*[1] and D. Rajesh[2]

[1*]Department of Electrical and Electronics Engineering, Government Polytechnic College, Nagercoil, Tamilnadu, India.
[2]Department of Computer Science Engineering, Satyam College of Engineering and Technology, Tamilnadu, India.

ABSTRACT

The important trouble of power efficient reliable routing is that it doesn't offer any back up mechanism for the failure of the nodes. The work of the paper predominant depends on the alternate direction supplied if the link got failure and to offer power efficient direction in between the network. It's going to lessen the time, price and increase the performance and the statistics price of the network. In wireless sensor networks, because of unreliable wireless media, host mobility and shortage of infrastructure, offering relaxed communications is bit tough in this kind of community environment. In present work to ensure the safety in unreliable mobile communication the cluster based totally topology technique is used, to reap confidentiality and authentication of nodes hash characteristic and MAC (Message Authentication Code) techniques are used in MWSN.

KEYWORDS

Cellular WSNs, Proposed protocol and Proposed algorithm.

Author for Correspondence:

Giji Kiruba D,
Department of Electrical and Electronics Engineering,
Government Polytechnic College,
Konam, Tamilnadu, India.

Email: d.jijikiruba@gmail.com

INTRODUCTION

A wireless sensor community (WSN) of spatially disbursed autonomous sensors to monitor bodily or environmental situations, which includes temperature, sound, stress, etc. And to ahead their data thru the nodes in network to a main server. The Implementation of WSN became inspired with the aid of military programs, they're used for battlefield surveillance. Now a days WSN networks are used for purchaser and industrial packages, additionally in business monitoring and manage of the process, monitoring of system health[2].

The WSN is constructed of "nodes" - from a few to numerous loads or maybe thousands, in which each node is connected to one (or now and again numerous) sensors. Every sensor node has commonly several parts: a radio transceiver with an inner antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and a power supply, commonly a battery or an embedded form of electricity harvesting. A sensor node length would possibly range from that of a shoebox down to the dimensions of a grain of dirt[11]. The price of sensor nodes is in addition variable, ranging from a few to masses of rupees, which relies upon on the complexity of the every character sensor nodes. Size and price constraints on sensor nodes bring about corresponding resources constrains consisting of strength, reminiscence, computational velocity and communications bandwidth. The topology of the WSNs can differ from a simple megastar network to a complicated multihop mobile network[5]. The navigation method among the hops of the community can be flooding or routing. Figure No.1 shows multi-hop mobile wireless sensor network.

The essential characteristics of a WSN encompass:

1. Power consumption parameter for nodes the usage of batteries or electricity harvesting[12].
2. Ability to handle with node screw ups.
3. Mobility of nodes.
4. Diversification of nodes.
5. Scalability to very massive scale of deployment.
6. Ability to deal with harsh environmental situations.
7. Ease of use.
8. Cross-layer layout.

PROBLEM IDENTIFICATION

The multihop routing in mobile sensor networks (WSNs) offers little protection in opposition to identification deception through replaying routing facts. An adversary can make the most this disorder to launch diverse dangerous or even devastating attacks against the routing protocols, together with sinkhole attacks, wormhole attacks, and Sybil attacks[4]. However the most distinguished works within the associated fields has been finished by Guoxing Zhan, Weisong Shi, et Al i.e. Design and Implementation of E^2R^2: A Trust-Aware Routing Framework for WSNs‖. Without tight time synchronization or regarded geographic statistics, E^2R^2 gives trustworthy and energy-efficient direction. Most importantly, E^2R^2proves powerful in opposition to those harmful attacks evolved out of identification deception; the resilience of E^2R^2 is tested via full-size evaluation with both simulation and emperical experiments on big-scale WSNs under various scenarios together with cell and RF-protecting network situations[6].

In E^2R^2 community desk is generate for direction selection where values are equal in appreciate to all nodes. How it may be efficient or maximum accurate routing of packets? These outcomes into growing give up to end put off. So efficient routing is important even as implementing framework. E^2R^2 also ignoring any packet level security and it becomes necessary to discover suitable safety because the facts may also consist of some touchy statistics which ought to now not be accessed through or can handiest be partially exposed to the general customers. So in the latest international, safety is a prime important difficulty, and encryption is one of the excellent alternative ways to make certain security. So while packet security has to consider in implementation of framework.

E^2R^2 wishes excessive packet transport rate. But hyperlink failure scenario is not considering. When packet comes to the node for forwarding, it makes a decision route by using agree with manager and neighborhood table. And if link failure occurs due to some purpose after deciding on direction for routing then packet loss is occurs. Due to this packet loss fee is will increase and packet transport fee decreases. This is all approximately E^2R^2 that is existing system for trust conscious routing and stopping identity deception assaults. Now for hyperlink failure resiliency, Srinivasan Ramasubramanian proposed Dual-Link Failure Resiliency through Backup Link Mutual Exclusion which classifies the processes to twin-link failure resiliency. BLME- Backup Link Mutual Exclusion is right methodology for hyperlink failure restoration[8]. BLME set of rules generates backup paths more before routing packets. If some hyperlink fails then that already generated backup path is used. And on this way hyperlink failure is recover. But if deeply observe backup route generation of BLME then it may be aware that BLME set of rules generates a whole lot of change paths at time earlier than from source to destination without want to any hyperlink failure arise. So in case while link failure does no longer occurs then these generated paths are waste in phrases of era time, computation fee as properly as it will increase postpone to packet reach at vacation spot. And in different case if link failure happens then also numbers of other paths are waste. Which have an effect on put off time and computation value. Proposed system robust framework for preventing identification deception assaults the use of backup direction era‖ is device which follows Trust conscious routing of E^2R^2 and advanced through together with packet protection, efficient routing technique for increasing packet transport rate. Integrated with BLME technique of backup course technology for hyperlink failure recovery for decreasing packet loss charge and End to End Delay and growing packet transport price which is also improve with green backup route generation for low computation value and minimum postpone[7].

Goals and Objective of E^2R^2 in particular guards a WSN in opposition to the attacks directing the multi-hop routing, specifically those based on theft through replaying the routing statistics. This device does not cope with the denial-of-carrier (DoS) attacks, in which an attacker intends to affect the community with the aid of using its aid. For example, we do not cope with the DoS assault of congestion community through resending several packets or bodily blocking the community[9]. E^2R^2 objectives to obtain the subsequent proper residences: High Packet delivery price, Energy Efficiency, scalability and flexibility. However, hyperlink failure situation is likewise taking into attention with the aid of E^2R^2. So, packet loss, time put off such matters happen because of link failure have to be don't forget whilst we need to achieve excessive throughput[1].

PROPOSED METHODOLOGY

In the proposed a novel power-conscious routing set of rules, referred to as reliable minimum power value routing (RMECR). RMECR finds energy efficient and reliable routes that increase the operational life of the community. RMECR is proposed for networks with hop-through-hop (HBH) retransmissions imparting hyperlink layer reliability, and networks with E2E retransmissions imparting E2E reliability. It considers the power consumption and the final battery electricity of nodes as well as first-class of links to find energy green and dependable routes that increase the operational life of the network[3].

Proposed Algorithm

A classifications of the sensor nodes in this paper, we divide the particularly-purposeful sensor nodes into three classes:

BN (Branch Node)

BNs are the only-hop pals of the BS. Each BN represents one department. The closer to the BS, the node has greater burdens on data transmission. The BN acts critical function inside the network, due to the fact as soon as it's exhausted the whole branch is separated and the downstream paths are correspondingly failed. In order to conserve electricity, the BN doesn't be part of the cluster formation and records sense. It just acts as a router in the community. Furthermore, if its energy is underneath a limitation value, it have to announce that it abandons the function of branch node and transforms to an everyday node.

CH (Cluster Head)

In our approach, cluster heads are elected distributed based totally at the parameters of the residual electricity and the range of buddies. CH is in charge of facts obtain, records process, facts aggregation and records transmission. The strength intake of CH is tons speedy than ordinary nodes.

SN (Substitute Node)

The substitute nodes for CHs. This strategy guarantees the records might be transmitted efficaciously even if the cluster head is exhausted. This ought to improve the reliability and fault tolerance of the gadget. The remained nodes are everyday nodes[8].

Process of ERCCR

The operation of ERCCR is split into exclusive rounds. The BS periodically collects the sensed facts and initializes a brand new spherical through sending a request message. In every round, ERCCR runs the subsequent 3 stages:

Phase one: Broadcast

This section starts from the BS broadcasting a request message. The layout of this message is REQ, RID, BID, SID, Ere, HCount, Eto, N, where REQ shows the type of message is request; RID is the spherical identifier, that is generated by means of the base station; BID is the identifier of the branch, i.e., identifier of the department node; SID is the identifier of the sender node; Ere is the residual electricity of the sender node; HCount is the hop counts from the sender to the base station; Eto indicts the general strength of all nodes, it's calculated by using the bottom station; Finally N is the sum of nodes after closing round. Here Eto and N are organized for the election of cluster heads. The BS to start with publicizes the message REQ, RID, F, BS, ∞, zero, Eto, N. After this phase, every node makes a decision whether it's miles a Branch Node, stores the parameters (Eto, N) for the following segment, and records the neighborhood facts, which affords a number one path and some opportunity paths to the BS. Each node rebroadcasts once and most effective once.

Phase Two: Cluster Formation

After preceding segment, each node has the information approximately the overall energy Eto and sum of nodes N. Each node comes to a decision whether or not to be a cluster head. Once the node has elected itself to be cluster head, it declares an advertisement message (ADV) the usage of a nonpersistent provider-feel multipath get admission to (CSMA) MAC protocol. Each non-cluster head node determines its cluster for this round by using deciding on the cluster head that requires the minimum conversation strength, primarily based on the obtained signal energy of the advertisement from every cluster head. After each node has decided to which cluster it belongs, it transmits a part of-request message (Join-REQ) returned to the chosen cluster head using a CSMA MAC protocol. The cluster head node units up a TDMA time table and transmits this agenda to the nodes within the cluster. Besides, if you want to improve the fault tolerance of the cluster, CH want elect one node as the unreal of the cluster head. CH will choose it from the nodes whose Join-REQ messages are heard by way of CH with the larger signal power, i.e., they may be towards CH than others. Then CH compares the power and neighbor quantity among these node, ultimately elects one node with higher parameters. CH sends a statement message (SNANN) to nodes. This message includes 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[10].

Phase Three: Data Propagation

This phase includes two steps: first the records propagation inside a cluster, then the statistics propagation from the cluster head to the BS, which is along multi-hops. In a cluster, nodes send their facts to the cluster head throughout their allotted transmission slot time. Once the cluster head receives all the facts, it plays facts aggregation to beautify the commonplace sign and reduce the uncorrelated noise amongst the indicators. In our approach, after every round, BS wishes to understand the entire residual power of all nodes and the sum of nodes alive. During this process, if the residual electricity of the cluster head is beneath a difficulty value Eurgent, it'll broadcast a strength-urgent assertion message, and ship the received data to the factitious node. The remaining nodes which haven't yet sent records change the cluster head correspondingly[13]. It's a completely dependable and flexible fault tolerant scheme. Then the ensuing statistics are despatched from the cluster head to the BS. Since the BS can be some distance away and the facts messages are massive, that is a multi-hop and high-electricity transmission. The cluster head firstly assessments its community. The node marked with discern‖ is the next hop and the path is the number one direction along it. Then CH constantly appears for the buddies with exceptional BID fee from its parent. After evaluating the electricity and variety of friends, the CH chooses the next hop nodes (multiple). After the following hop nodes are chosen, the CH (intermediate node) transmits data alongside the primary route at the beginning. If the information is correctly sent to the following hop, the next hop will response a SUCCEED message. After a positive threshold time, if CH didn't get the reaction message, it'll ship the facts alongside every other subsequent hop. The message sent from CH includes message kind (DATA), subsequent hop ID, BID, aggregated facts, Ncluster and Ecluster. For inter-media nodes, it checks the BID, reveals next hop with the equal BID in its neighbors and transmits facts to it. Similar to ultimate step, it waits SUCCEED message from the subsequent hop for a certain threshold time. If it may't get the response message, it will send a FAILURE message back to its ultimate hop. If any inter-media node gets the FAILURE message, it'll notice its final hop till CH gets the facts.

Algorithm 1

Initially BS collects data regarding of all the nodes within the community.

- BS transmit message to all nodes in the network.

Assigning energy to all nodes.

Choose the source and destination.

To find the neighbours.

- First locate HBH transmission.
- If this course is reliable then E2E course is dependable.

Choose the shortest routing the use of Dijkstra's set of rules.

- Dijkstra's set of rules is simplest heuristic answer for find minimum power fee route.
- $C(P(s,v))=C(P(s,v))+W(u,v)$

Calculating the minimum electricity routing route for using MinMax set of rules.

Sending packets via the dependable direction.

Security in key Distribution

Here considers a cluster-based ad hoc hierarchical network topology. A subset of the community nodes is decided on to function the community spine over which vital network manage features are supported. The approach to topology manipulate is often called clustering, and consists of choosing a set of cluster heads in a manner that each node is related to a c1uster head, and c1usterheads are related with one another directly or via gateways ,in order that the union of gateways and c1usterheads constitute a connected spine. Once elected, the cluster heads and the gateways assist reduce the complexity of retaining topology statistics, and can simplify such important functions as routing, bandwidth allocation, channel get right of entry to, power manipulate or digital-circuit help. The fundamental steps for achieving the comparative evaluation are given under.

Turn on Tracing Window

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

Turn on Tracing Window

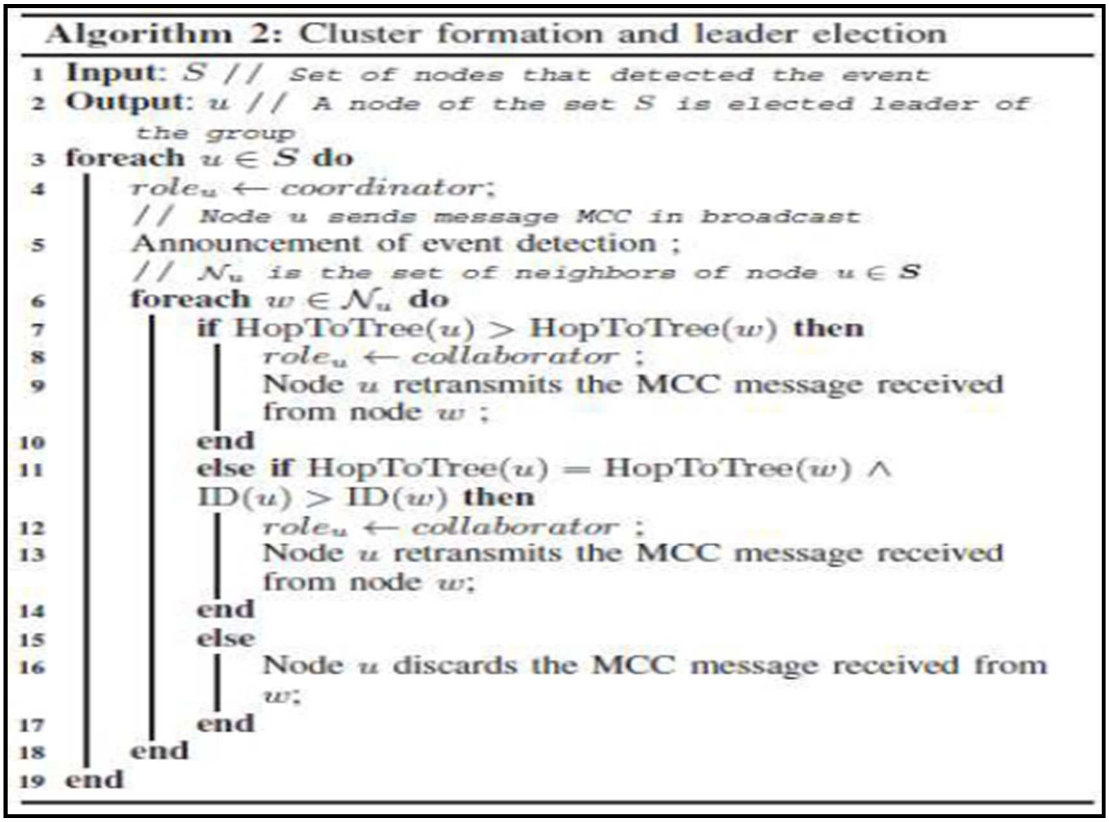
The next step is to present topology for the community. For the WANET, the desired topology is MESH. For any wireless network, it's far important to provide all the necessary parameters like kind of channel, kind of advert-hoc routing protocol, kind of antenna, and so forth.

Turn on Tracing Window

This section will create an appropriate routing marketers for the records drift. In WANET, TCP has been used. It is plenty greater dependable than the opposite and its miles the only which has been supported easily with the aid of NS-2. It offers the routing algorithm for the network.

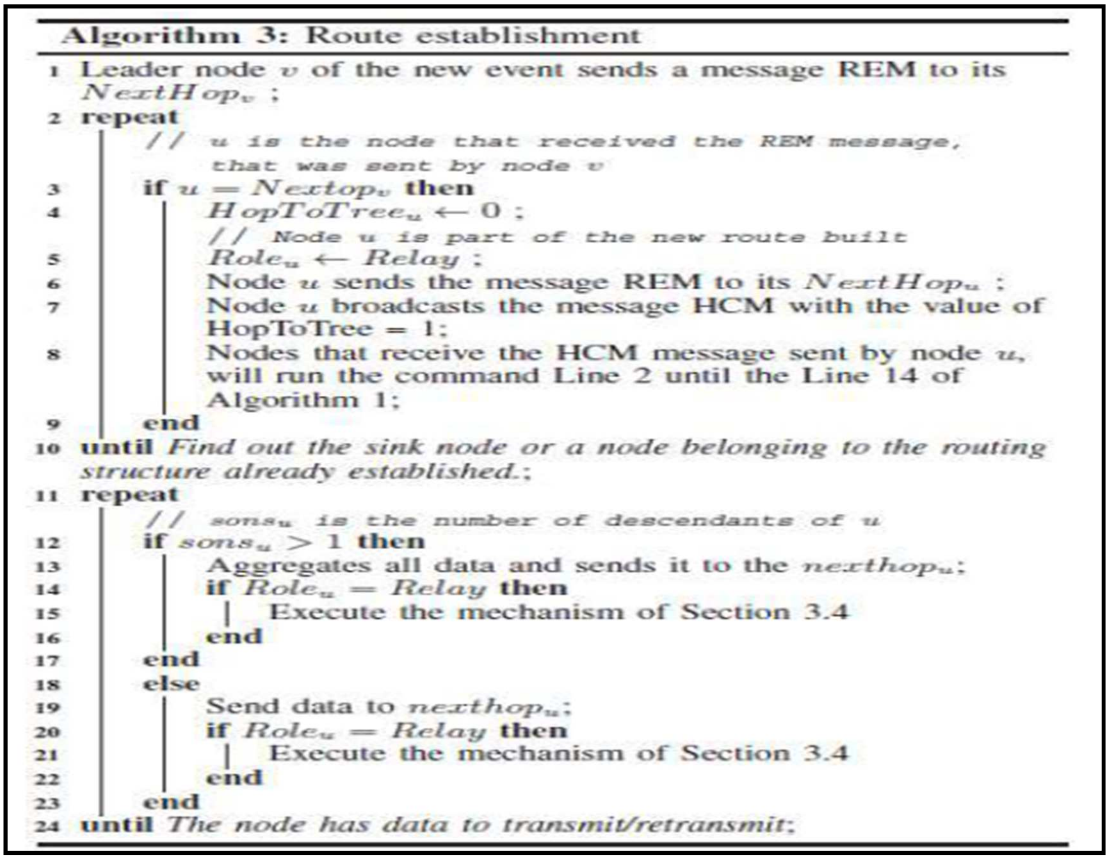
Turn on Tracing Window

The script would possibly create a few output on stdout, it would write a hint report or it might start call to visualize the simulation. It is a discrete occasion simulator and very much beneficial for evaluation of dynamic nature of communication community[4]. The pictorial representation of set of rules shown in Figure No.1.



Algorithm 2: Cluster formation and leader election

```
Input: $S$ // Set of nodes that detected the event
Output: $u$ // A node of the set $S$ is elected leader of
    the group
foreach $u \in S$ do
    $role_u \leftarrow coordinator$;
    // Node u sends message MCC in broadcast
    Announcement of event detection ;
    // $\mathcal{N}_u$ is the set of neighbors of node $u \in S$
    foreach $w \in \mathcal{N}_u$ do
        if HopToTree($u$) > HopToTree($w$) then
            $role_u \leftarrow collaborator$ ;
            Node $u$ retransmits the MCC message received
            from node $w$ ;
        end
        else if HopToTree($u$) = HopToTree($w$) $\wedge$
        ID($u$) > ID($w$) then
            $role_u \leftarrow collaborator$ ;
            Node $u$ retransmits the MCC message received
            from node $w$;
        end
        else
            Node $u$ discards the MCC message received from
            $w$;
        end
    end
end
```



Algorithm 3: Route establishment

```
Leader node $v$ of the new event sends a message REM to its
$NextHop_v$ ;
repeat
    // $u$ is the node that received the REM message,
       that was sent by node $v$
    if $u = Nextop_v$ then
        $HopToTree_u \leftarrow 0$ ;
        // Node $u$ is part of the new route built
        $Role_u \leftarrow Relay$ ;
        Node $u$ sends the message REM to its $NextHop_u$ ;
        Node $u$ broadcasts the message HCM with the value of
        HopToTree = 1;
        Nodes that receive the HCM message sent by node $u$,
        will run the command Line 2 until the Line 14 of
        Algorithm 1;
    end
until Find out the sink node or a node belonging to the routing
structure already established.;
repeat
    // $sons_u$ is the number of descendants of $u$
    if $sons_u > 1$ then
        Aggregates all data and sends it to the $nexthop_u$;
        if $Role_u = Relay$ then
            Execute the mechanism of Section 3.4
        end
    end
    else
        Send data to $nexthop_u$;
        if $Role_u = Relay$ then
            Execute the mechanism of Section 3.4
        end
    end
until The node has data to transmit/retransmit;
```

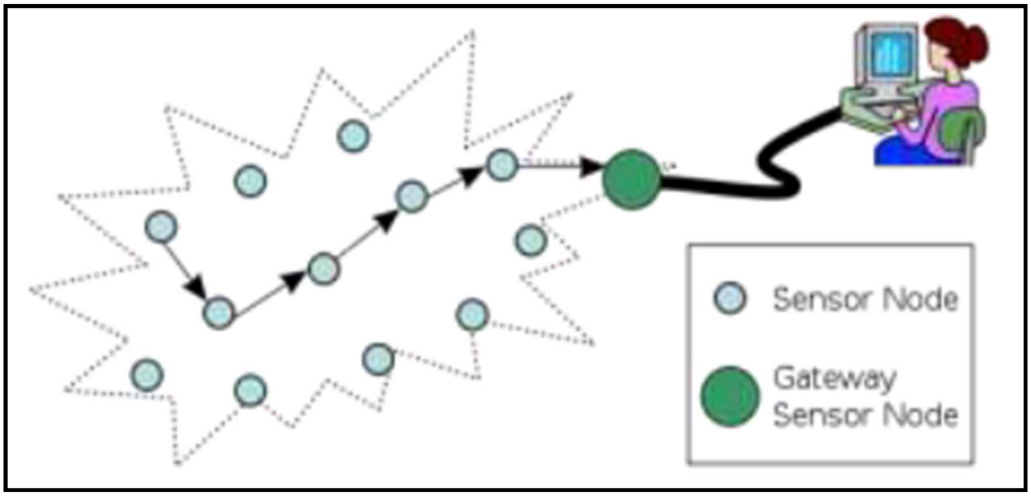


Figure No.1. Typical Multihop Mobile Wireless Sensor Network

SIMULATION RESULTS

Figure No.2: shows the packet deliver ratio of mobile wireless sensor network

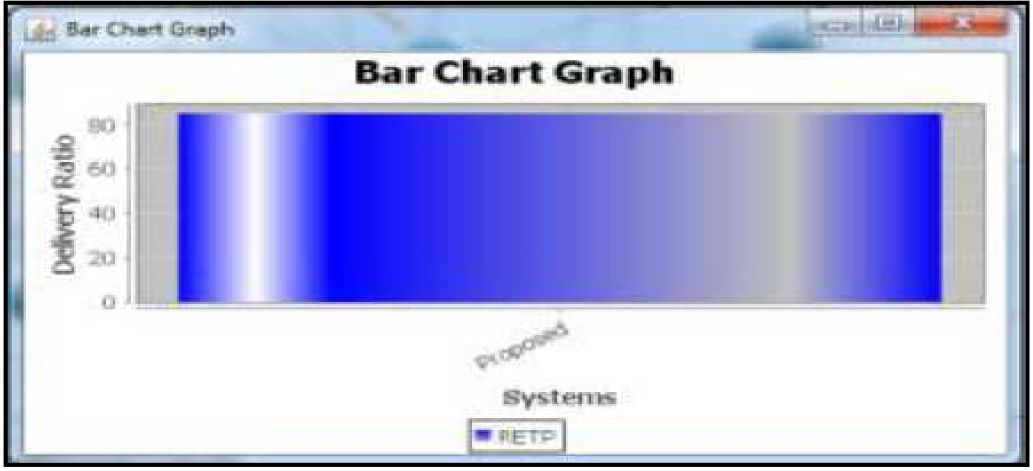


Figure No.2: Packet Delivery Ratio

Figure No.3: shows the energy efficiency of mobile wireless sensor network

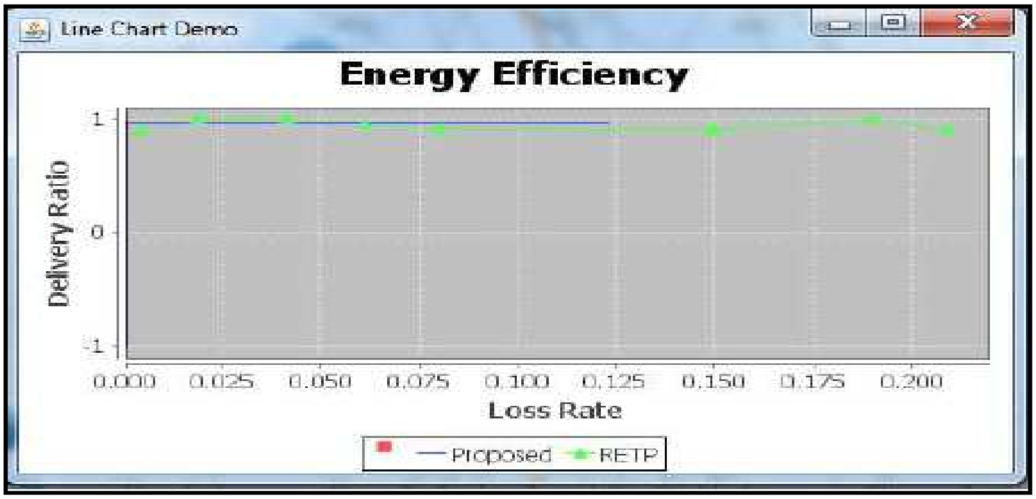


Figure No.3: Energy Efficiency

Figure No.4: shows the cost of mobile wireless sensor network

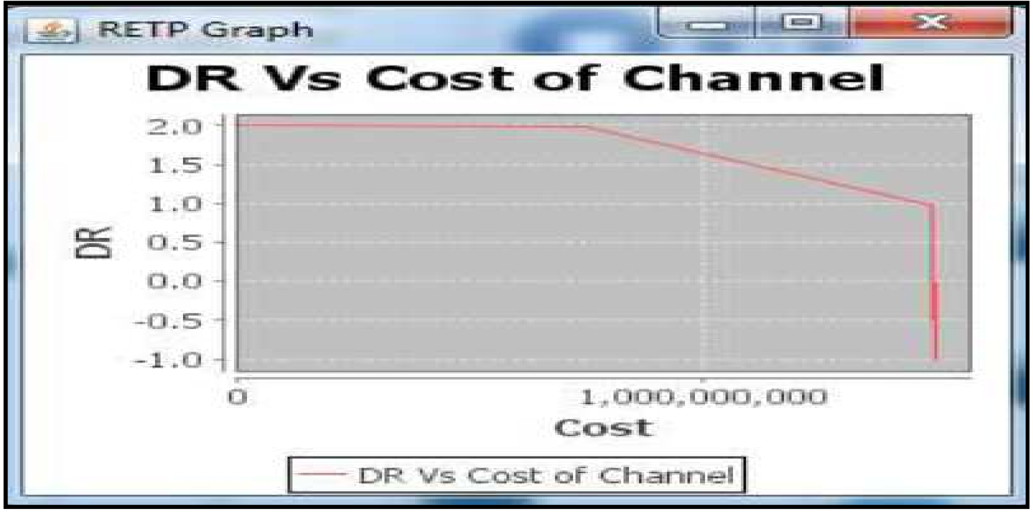


Figure No.4: DR vs cost of Channel

Figure No.5: shows the energy efficiency of mobile wireless sensor network

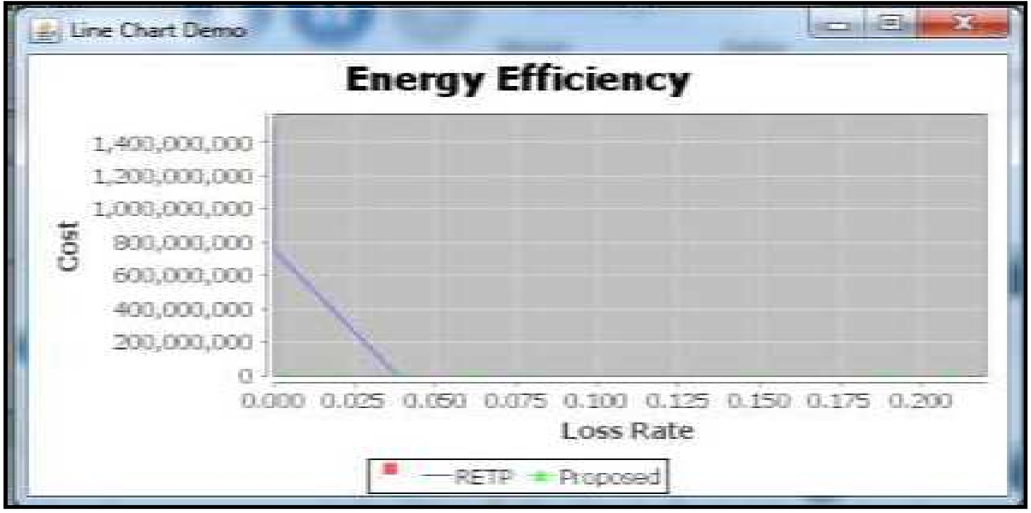


Figure No.5: Energy Efficiency

CONCLUSION

In this paper, we have implemented a power-green and reliable routing protocol for cellular WSNs. The proposed protocol E^2R^2 is hybrid cluster based. This protocol provides power green routing in among the network, it also offer the backup course if the node were given failure even as sending statistics from one node to any other. It additionally provide the security for the information which is going to be ship. By means of selecting the trade direction while the node were given failure power green and reliable course may be selected. The proposed protocol has additionally been examined below the effect of noticeably mobile sensor nodes and consistent with outcomes we can conclude that the proposed algorithm have high throughput even in excessive statistics fee, excessive mobility and in addition it offers high security to facts. In future it would be interested to put in force proposed algorithm in real international situation.

ACKNOWLEDGEMENT

The authors wish to express their sincere gratitude to Department of Electrical and Electronics Engineering, Government Polytechnic College, Nagercoil, Tamilnadu, India for providing necessary facilities to carry out this research work.

CONFLICT OF INTEREST

We declare that we have no conflict of interest.

BIBLIOGRAPHY

1. Mohammad Masdari and Maryam Tanabi. Multipath Routing protocols in Wireless Sensor Networks: A Survey and Analysis, *International Journal of Future Generation Communication and Networking,* 6(6) 2013, 181-192.
2. Pushpa S, Elias S, Easwarakumar K S, Maamar Z. Referral based expertise search system in a time evolving social network, *Proceedings of the third Annual ACM Bangalore Conference,* ISBN: 978-1-4503-0001-8, 2010.
3. Ali Norouzi, Faezeh Sadat Babamir, Abdul Halim Zaim. A Novel Energy Efficient Routing Protocol in Wireless Sensor Networks, *IEEE,* 3(10), 2011, 341-350.
4. Pushpa S, Easwarakumar K. Exploring the Influence of Time-Sensitive and Unsupervised Learning of Topic-Specific Information in Citation Analysis, *European Journal of Scientific Research,* 67(3), 2012, 474-485.
5. 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*, ISBN: 978-1-4577-0974-6, 2011.
6. Satvir Singh, Meenaxi. A Survey on Energy Efficient Routing in Wireless Sensor Networks, *IEEE,* ISBN: 978-1-4799-3926-8, 3(7), 2013.
7. 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, 1(6), 2013.
8. Monica Mundada R, Savan Kiran, Shivanand Khobanna, Raja Nahusha Varsha and Seira Ann George. A study on energy efficient routing protocols in wireless sensor networks, *International Journal of Distributed and Parallel Systems (IJDPS),* 3(3), 2012, 311-330.
9. Rajesh D, Firoja Banu M, Stella D, Ansila Grace P. Ch Panel Based Routing Scheme for Mobile Wireless Sensor Network, *International Journal of MC Square Scientific Research,* 8(1), 2016, 183-198.
10. Kalpana G, Bhuvaneswari T, A Survey on Energy Efficient Routing Protocols for Wireless Sensor Networks, *2nd National Conference on Information and Communication Technology (NCICT),* 2011, 12-18.
11. Vinoth Kumar K, Karthikeyan S. Multihop Energy Efficient Reliable and Fault Tolerant Routing Protocol for Wireless Sensor Networks, *International Journal of Emerging Technology and Advanced Engineering,* 3(2), 2013, 395-409.
12. Allam Balaram, Pushpa S. A Robust Location Privacy in Vehicular Ad Hoc Networks, *International Journal of Applied Engineering Research,* 10(17), 2015, 13135-13141.
13. Rajesh D, Keiser Jahana S, Sivakalai R, Jasmin Meera Banu P. Detection and isolation of attacks in manet using ts-aomdv, *International Journal of MC Square Scientific Research*, 8(1), 2016, 170-182.

Please cite this article in press as: Giji Kiruba D and Rajesh D. Energy resourceful and consistent clustered routing for mobile wireless sensor networks, *International Journal of Engineering and Robot Technology,* 4(2), 2017, 49-57.