International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 14 (2015) pp 34799-34805

Reliable Multicast Routing based on Energy for Wireless Sensor Networks

[1]M.Balamurugan, [2] Dr.R.Poongodi

[1]Research Scholar, Karpagam University, Coimbatore, India
[2]Department of ECE, PPG Institute of Technology, Coimbatore, India
E-mail: sabaalu@gmail.com

Abstract:
Wireless sensor network (WSN) has recently become promising network architecture and is widely used in many applications, including environmental monitoring, object detection, event tracking, and security surveillance. In WSNs, nodes in the area of interest must report sensing readings to the sink, and this report always satisfies the report frequency required by the sink. Reliable multicast routing is proposed for achieving an energy-efficient and reliable routing path. It consists of four phases. In first phase, the cluster routing is established to ensure load balancing and longer network lifetime. In second phase, secure multicast routing is deployed with clustering to provide data packet integrity. In third phase, the energy consumption of wireless sensor nodes are determined. In this phase, the energy consumption threshold model is developed. By simulation results, the proposed RMR achieves less end to end delay, better packet delivery ratio, less overhead, less end to end delay and energy consumption in terms of mobility, speed, simulation time, time and number of nodes than the existing scheme LTDMS and HDTMP.

Keywords - WSN, RMR, Multicast routing, energy consumption, Node join and leave, cluster head election, delay, and packet delivery ratio.

I. INTRODUCTION

A. Wireless Sensor Networks (WSNs)

A Wireless Sensor Network (WSN) consists of a number of sensor nodes, which are limited in terms of energy, CPU power, and memory. On the sensor nodes may run different applications for different tasks such as event detection, localization, tracking, and monitoring. Such applications should be configured and updated during the life-time of the sensor nodes and over the network. An update with many unicast connections to the nodes is very inefficient and consumes resources such as bandwidth and energy. Thus it is obvious that multicast communication the management of WSNs may benefit by reducing the number of transmitted packets and by saving energy. To access WSNs via the Internet, a IP-based communication is required. Thus multicast communication should be IP-based as well.

B. Design goals of Wireless Sensor Networks WSNs)

Based on the application, different architecture, goals and constraints have been considered for WSNs. The following design goals of Wireless Sensor Networks are given below.

a. Energy Considerations

During the creation of an infrastructure, the process of setting up the routes is greatly influenced by energy considerations. Since the transmission power of a wireless radio is proportional to distance squared or even higher order in the presence of obstacles, multihop routing will consume less energy than direct communication. However, multi-hop routing introduces significant overhead for topology management and medium access control. Direct routing would perform well enough if all the nodes were very close to the sink. Most of the time sensors are scattered randomly over an area of interest and multi-hop routing becomes unavoidable.

b. Node deployment

Node deployment in WSN is application dependent and affects the performance of the routing protocol. The deployment can be either deterministic or randomized. In deterministic deployment, the sensors are manually placed and data is routed through pre-determined paths; but in random node deployment, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner. Hence, random deployment raises several issues as coverage, optimal clustering etc. which need to be addressed.

c. Energy consumption without losing accuracy

Sensor nodes can use up their limited supply of energy performing computations and transmitting information in a wireless environment. As such, energy conserving forms of communication and computation are essential. Sensor node lifetime shows a strong dependence on the battery lifetime. In a multi-hop WSN, each node plays a dual role as data sender and data router. The malfunctioning of some sensor nodes due to power failure can cause significant topological changes and might require rerouting of packets and reorganization of the network.

II. RELATED WORK

Lu su et.al [1] proposed an energy optimal multicast routing protocol for wireless sensor networks. The protocol does not pose any restriction on synchronization between neighboring nodes. Each node only needs to know the relative position of its neighbor's working period. The multicast tree was constructed based on predefined delay bound. But this protocol does not provide improved packet delivery rate and not satisfied the end to end packet delivery delay.

Ashok babu et.al [2] proposed a basic ant-based routing algorithm and several improvements, inspired by the features of wireless networks were considered and implemented. The resulting routing protocol, called Energy-Efficient Ant Based Routing uses lightweight ants to find routing paths between the sensor nodes and the sink nodes, which are optimized in terms of distance and energy levels. These special ants minimize communication loads and maximize energy savings, contributing to expand the lifetime of the wireless network.

Leiwang et.al [3] proposed proposes a multi-rate network coding scheme to improve the energy efficiency of WSNs. This scheme can improve energy efficiency on three aspects: firstly, it can reduce the number of intermediate nodes in which re-encoding operation is required, thus reducing the number of required transmission links; secondly, it can make maximal data fusion with the original packets, which ensures that more data can be sent to receivers in a transmission period; thirdly, this scheme can work on a very small finite field, which indicates that the computation overhead of network coding is low.

Zhi-jie Han et.al [4] proposed the algorithm is for sensor networks. Based on the geographic routing algorithms, k-redundant multicast graph was constructed. The network throughput and bandwidth utilization were improved, the effect of minimum cut to maximum flow was determined, and the network multicast routing performance was enhanced by utilizing the network coding mechanism.

Mohan Kumar et.al [5] developed a trust system based on trust policy. The trust policies are formulated based on the node properties. Unlike the existing work, we have used composite trust metric for evaluating the trust of nodes in sensor application on the basis of social trust in addition to traditional QOS. As an application of the proposed trusted routing algorithm, we introduce trust source routing protocol on the basis of novel reactive routing protocol (using MAC algorithm). In addition to this trust system, we also provide data security using MAC authentication using shared secret key to perform the cryptographic function.

Fengjun et.al [6] proposed an advanced multiple-hop routing protocol named LEACH-L, whose features can be described as follows: when the cluster-heads are close to, they directly communicate with Base station (BS); when they are far in distance, they telecommunicate by multiple-hop way, and the shortest transmission distance is limited. The sensors in different areas use different frequencies and gaps to communicate with BS.

Mohsen Nejadkheirallah [7] proposed multi tracking fuzzy method with the capability of supporting the sink has been introduced. The fuzzy logic has been used for choosing a node and as a relay to transfer the data to the sink. The main feature of this method is that the increase in the number of the nodes and sinks does not have an undesirable effect on the efficiency of the network and as a result this protocol enjoys a good measurability.

Stefanos A. Nikolidakis et.al [8] proposed a novel energy efficient routing protocol. It selects cluster heads in the network using a model, as most of the previously proposed protocols. However, the main difference with other protocols is that this one uses a more efficient mechanism to elect a node as the cluster head. This is performed by considering the current and the estimated future residual energy of the nodes, along with the number of rounds that they can be cluster heads, in order to maximize the network lifetime. ECHERP models the network and the energy spent by the nodes as a linear system and, using the Gaussian elimination algorithm, selects the cluster heads of the network.

Kyuhong Lee and Heesang Lee [9] proposed an energy-efficient self-organized clustering model with splitting and merging (EECSM), which performs clustering and then splits and merges clusters for energy-efficient cluster-based routing. EECSM uses information of the energy state of sensor nodes, in order to reduce energy consumption and maintain load balance. We show the validity of splitting and merging of clusters and then compare the performance of the proposed EECSM with that of a well-known cluster-based self-organization routing protocol for WSNs. The proposed model attempts to maximize the network lifetime and maintain load balance through the selection of CHs and by resizing clusters through combined techniques of advantages of self-organized protocols and cluster-based routing. Since EECSM uses a self-organizing approach, it has good characteristics, such as distributed control, adaptability, robustness, and scalability.

Min yoon et.al [10] proposed a new energy-efficient routing scheme based-on cluster. In our scheme, we design a new cluster head selection algorithm based on node connectivity and devise cluster split and merge algorithms to conduct the optimal clusters from initial clusters. Message success rate was used which is one of the popular measures for data communication reliability, to guarantee data communication reliability for network. To reduce data communication overhead, it is used the only information of neighbor nodes at both cluster construction and cluster head selection

Mohammad S. Obaidat et.al [11] proposed Dynamic Energy Efficient and Secure Routing Protocol.This protocol is used for securing the wireless sensor networks and is based on Ant colony optimization (ACO). It uses quality-of-service (QoS) and reputation to find out the trust of the node. Thus, by monitoring these two parameters the protocol is able to detect and disable the malicious nodes from gaining access and participating in the network.

P.Sivaranjanadevi, and T.Poongothai [12] proposed Energy Efficient Routing and Fault node Replacement (EERFNR) Algorithm to increase the lifetime of wireless sensor network, reduce data loss and also reduce sensor node replacement cost. Transmission problem and sensor node loading problem is solved by adding several relay nodes and arranging sensor node's routing using Hierarchical Gradient Diffusion. The Sensor node can save some backup nodes to reduce the energy for re-looking the route when the sensor node routing is broken.

Xiao-Hui Li and Zhi-Hong Gua [13] proposed an energy-aware dynamic routing strategy in order to provide balanced energy consumption in wireless sensor networks, hence, prolonging the lifetime of the network. The proposed routing algorithm uses local betweenness centrality to estimate the energy consumption of the neighboring nodes around a given local sensor node, without requiring global information about the network topology or energy consumption, and to divert traffic from nodes that aremore heavily used. Because nodes with large local betweenness centrality consume energy more

quickly, the network lifetime can be prolonged by redistributing energy consumption to nodes with smaller local betweenness centrality.

Kyuhong Lee and Heesang Lee [14] proposed an energy-efficient self-organized clustering model, the so-called EECSM.The proposed model attempts to maximize the network lifetime and maintain load balance through the selection of CHs and by resizing clusters through combined techniques of advantages of self-organized protocols and cluster-based routing. Since it uses a self-organizing approach, it has good characteristics, such as distributed control, adaptability, robustness, and scalability. Moreover, it can decide on the proper CHs for energy efficiency. It can also resize clusters for maintaining a suitable size, and further it can also restore damaged clusters on its own, based on local information.

Hamid reza Hassaniasl et.al [15] proposed Score-Aware Routing Algorithm (SARA) is used to enhance routing quality. For that, they have analyzed the five factors like distance between each node and sink, number of observed sources by each node, remaining energy in each node and reliability of communication link and value of traffic in each node. It was more efficient in terms of decreasing delay, decreasing the number of lost packets, improving the load distribution and purposeful network lifetime. It was shown that with higher network density or higher number of sources and higher rate of sent data, the efficiency of the developed algorithm would increase, and such increase is due to the higher number of nodes suitable for selection for routing.

Yuxin Mao and Guiyi Wei [16] proposed a novel approach of secure data collection for wireless sensor networks. They explored secret sharing and multipath routing to achieve secure data collection in wireless sensor network with compromised nodes. They presented a novel tracing-feedback mechanism, which makes full use of the routing functionality of wireless sensor networks, to improve the quality of data collection. The major advantage of the approach is that the secure paths are constructed as a by-product of data collection. The process of secure routing causes little overhead to the sensor nodes in the network. Compared with existing works, the algorithms of the proposed approach are easy to implement and execute in resource-constrained wireless sensor networks.

K. Vanaja and R. Umarani [17] deals with the fault management to resolve the mobility induced link break. The proposed protocol is the adaptive fault tolerant multipath routing (AFTMR) protocol which reduces the packet loss due to mobility induced link break. In this fault tolerant protocol, battery power and residual energy are taken into account to determine multiple disjoint routes to every active destination. When there is link break in the existing path, AFTMR initiates Local Route Recovery Process.

The paper is organized as follows. The Section 1 describes introduction about WSNs, goals and issues. Section 2 deals with the previous work which is related to energy efficient and secure routing algorithms. Section 3 is devoted for the implementation of proposed scheme. Section 4 describes the performance analysis and the last section concludes the work.

III. IMPLEMENTATION OF PROPOSED SCHEME

In the proposed model, cluster is constructed based on the recommendation from the neighbor nodes. Cluster head is chosen based on the battery level. If the energy falls below the threshold value, a new cluster head election message will be sent to all the nodes inside the cluster region. Node joining and node leaving procedure are also proposed in the cluster methodology. A secure multicast group is introduced with encryption scheme to ensure authentication. Along with this, a new energy model is illustrated to ensure more network lifetime. The following phases describe the proposed model.

I. Cluster Group Operation

A. Establishing a cluster region

In the proposed cluster region, each mobile node communicated with each other. Nodes recommend one of its neighbor mobile nodes as a cluster head and forming a cluster region. If it is continued, cluster head and its neighbor recommenders form a one hop range cluster. Once the mobile node recommends a cluster head, it sends to the cluster head a recommend message that includes proposal certificates (P_Certificate). These certificates are used to authenticate whether the cluster head has many cluster members that trust the head. The following are a cluster head recommend message and proposal certificates.

Recommend Message:

M(Mobile $node_1$'s id, Mobile $node_2$'s id, Mobile $node_2$'s trust value, P_Certificates, "recommend message");

Proposal Certificate (P_Certificate):

{Mobile $node_1$'s id, Mobile $node_2$'s id, generate time, confirmation, "Recommend", $node_1$'s PUB_KEY, signature (Mobile $node_1$'s id, Mobile $node_2$'s id, generate time, confirmation, "Recommend")}

B. Cluster head election

Once the cluster regions are formed, the cluster head schedules the transmission of each member in a time division multiplexing manner and inform all the cluster members. Cluster heads are chosen based on battery power level. Cluster head maintains the cluster routing table and cluster members routing table. All the cluster members monitor the status of cluster head power level. When the current cluster head's battery power level falls below a predetermined threshold or serve for a fixed period of time, it broadcasts a new cluster head election message request will be sent to all the cluster members. All the nodes then vote for a new cluster head using certification secret ballot. It can be done by replying to the *new cluster head election* message with its choice of candidate. The reply message is encrypted with the pair wise key with the cluster head. Neighbors therefore have no idea of the political affiliation of each other since the key is private and, different for each node–cluster head pair. The current cluster head then counts the votes and decides the winner based on high battery power level. The node with the second highest number of votes and battery level is selected as the vice cluster head. The purpose of the vice cluster head is to assume cluster head function in the event that the newly elected cluster head fails before handing over to its successor.

At the completion of counting, the cluster head multicast the winner and runner-up to all the members of the cluster.
For greater integrity and authentication the new winner and runner-up have to pass a challenge-response from the cluster head before they are allowed to take in-charge. The corrupt nodes are blacklisted in the cluster nodes' routing tables by setting its trust level value to -1. Once a cluster member node is set to -1 no further trust level update is done.

C. Cluster member Join operation

In the proposed cluster region, node join operation is executed in two cases. One is when a node first enters into the network. Another is the case when a node moves from one cluster to another cluster. In the first case, the cluster head has to evaluate the node's proposal value from scratch because the node does not have a proposal certificates. In the second case, an incoming mobile node gives to the new cluster head the proposal certificates that are received from the previous cluster head. Using these certificates, the new cluster head authenticates and establishes an initial proposal value of the new member node without its own experience. The join operation is carried out as follows. First, a node broadcasts a route request hello message. Any cluster head that receives the message sends a respond message to the node. The respond message of the head contains the number of member nodes. Second, after receiving the response message from the cluster head, the joining node sends to the cluster head. The cluster member join message shown below.

Cluster member Join Message:

M(Mobile node$_1$'s id, cluster head's id, previous cluster head's id, P_Certificates, "cluster member join message")

If there are more than two cluster heads in the neighborhood, the joining mobile node selects one cluster head that has more cluster members than the other cluster heads. Third, after the cluster head receives a cluster member join message, it evaluates the proposal value of the joining node by referring to the previous proposal value certified by the previous cluster head. If the joining node is not able to find any cluster head in a one-hop range, the node extends the search area to a two-hop range. If there is no cluster head in a two-hop range, then the joining node has to reconstruct the cluster with the neighbor nodes.

D. Cluster member Leaving Operation

In the cluster region, cluster member can leave a group in a different ways. The most straightforward case is when a mobile node wants to leave and it does not have any member children. Let's assume any cluster member is now leaving the group. The following ways illustrate the cluster member leaving:

Lively Leaving:
A node notifies its parent node of leaving before it moves or runs out of battery power.

Submissive Leaving:
A node fails silently due to hardware failure or physical damage and does not notify its parent.

In all two cases, the local parent node generates a new level pair wise key and multicasts it to its member children. After this update, the node that just left can no longer decrypt group messages and this guarantees forward secrecy for multicast. In the case of lively leaving, if the leaving node has no children, it can simply leave the group without any other issues. However, when a cluster member leaves the group, this leaves a break in the level structure and multicast tree path. To repair the multicast tree structure, leaving node's logical parent to become the parent of the leaving node's children. Once this broken level is bridged, no effects will happen above the leaving node's parent or below the leaving node's children.

II. Secure Multicast Group Formation

In the proposed secure multicast, hop by hop encryption is adopted. Packet is multicasted with its level key. Each member node that is a logical child of the cluster head will then decrypt the message. If the member node receiving the packet is a parent of a subsequent level, the node will re-encrypt the message using its parent level key and send the message onto each of its children. The packet format is given as,

Cluster group ID + MAC ID+ Seq.No+ Message

At each level the packet will be decrypted and re-encrypted with the next level's keys before being sent on. An alternative would be to have the cluster head generates a random key, *K*, and encrypt the message with this key. At each level, the parent decrypts and re-encrypts *K*, but not the entire message. This would speed propagation of the message by saving us from having to decrypt and re-encrypt the entire message at every level during packet forwarding.

III. Energy Model

In the proposed energy consumption model, the residual of the entire network is expressed in terms of relationship among consumed and initial energy. Residual or remaining energy is defined by consumed energy in $\Delta\tau$ from the battery power in $\tau - \Delta\tau$.

$$E_{remainingk}(\tau) = E_{initial,k}(\tau - \Delta\tau) - E_{consumed,k}(\Delta\tau) \quad (1)$$

$$E(\Delta\tau) = \frac{\partial E}{\partial \tau}(\Delta\tau) \quad (2)$$

$$\Delta\tau = \tau_2 - \tau_1$$

A nonlinear relationship is anticipated between the overall energy consumption of the system and its constituents based on network design. A simpler linear approach is adopted to model the overall energy consumption and explore the implication. The following overall energy is expressed as a linear combination of sensor node units namely memory unit, process unit, active state unit.

$$E_{consumedk}(\Delta\tau) = \lambda_1 E_{individual,k}(\Delta\tau) + \lambda_2 E_{local,k}(\Delta\tau) + \lambda_3 E_{active,k}(\Delta\tau) + \lambda_4 E_{battery,k}(\Delta\tau) + \lambda_5 E_{\sin k,k}(\Delta\tau) \quad (3)$$

IV. PERFORMANCE ANALYSIS

We use Network Simulator (NS2) to simulate our proposed algorithm. Network Simulator-2(NS2) is used in this work for simulation.NS2 is one of the best simulation tools available for Wireless sensor Networks. We can easily implement the designed protocols either by using the otcl coding or by writing the C++ Program. In either way, the tool helps to prove our theory analytically.

In our simulation, 200 mobile nodes move in a 1000 meter x 1000 meter square region for 60 seconds simulation time. All nodes have the same transmission range of 250 meters. Our simulation settings and parameters are summarized in table 2.

Table2. Simulation settings and parameters of proposed algorithm.

No. of Nodes	200
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	60 sec
Traffic Source	CBR
Packet Size	80 bytes
Mobility Model	Random Way Point
Transmitter Amplifier	150 pJ/bit/m^2
Package rate	4 pkt/s
Protocol	LEACH

A. 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.

Path Reliability Rate:

It is defined as to ensure path has never been corrupted or broken.

Overhead:

It means that ratio of number of routing control packets to the normalized packets.

Throughput:

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

The simulation results are presented in the next part. We compare our proposed algorithm RMR with our previous scheme LTDMS and HDTMP in presence of energy consumption.

Figure 3 shows the results of energy consumption for varying number of nodes from 10 to 200. From the results, we can see that RMR scheme has minimal energy consumption than the LTDMS and HDTMP scheme.

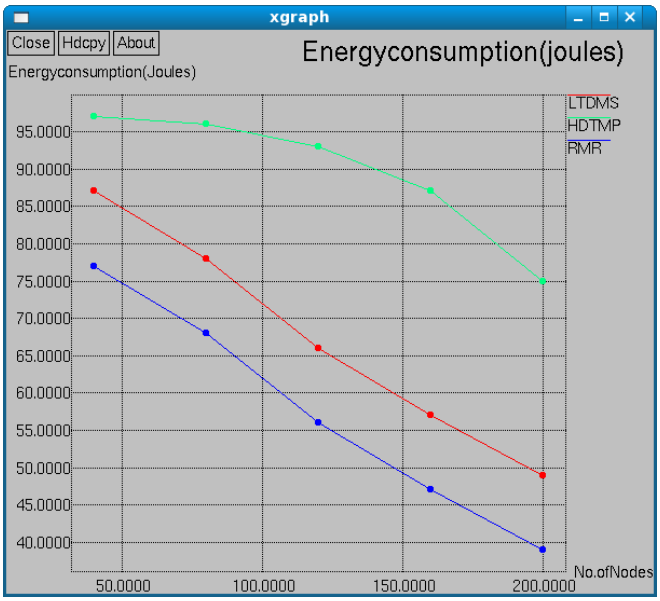

Fig. 3. Time Vs Energy consumption

Fig. 4, presents the Delivery ratio for RMR, LTDMS and HDTMP. It is clearly seen that number of packets delivered by RMR is high compared to LTDMS and HDTMP.

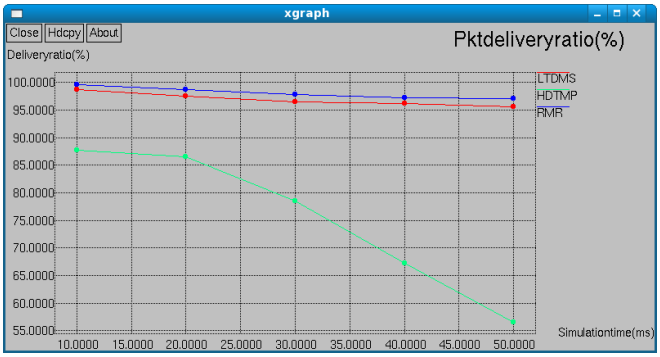

Fig. 4. Simulation time Vs Packet Delivery Ratio

Fig. 5, presents the comparison of authentication rate. It is clearly shown that the authentication rate of RMR is higher than LTDMS and HDTMP.

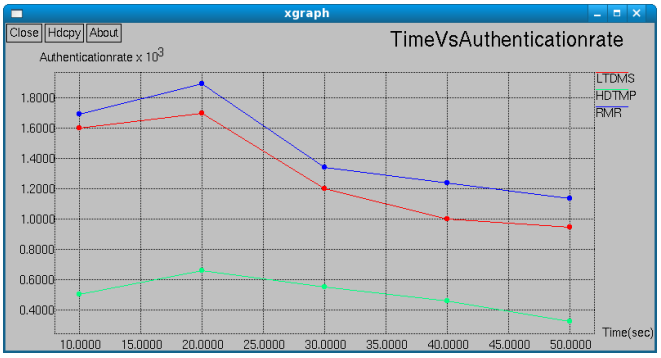

Fig. 5. Time Vs Authentication rate

Figure 6 shows the results of Mobility Vs End to end delay. From the results, we can see that RMR scheme has slightly lower delay than the LTDMS and HDTMP scheme because of authentication routes.

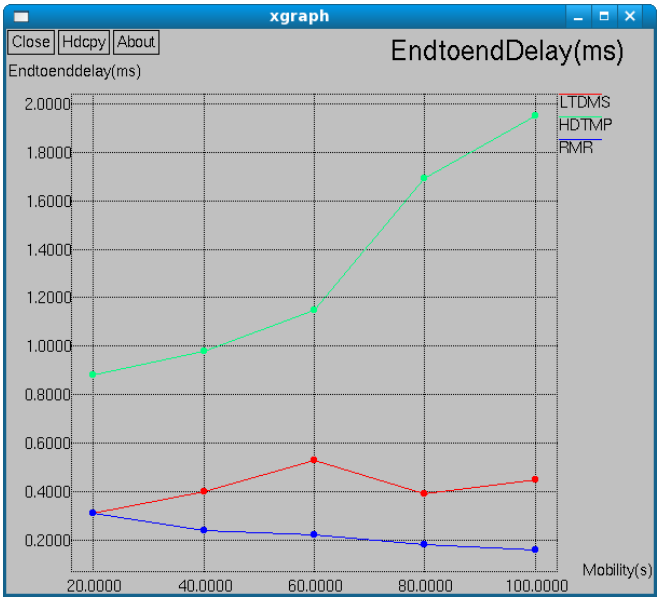

Fig. 6. Speed Vs End to end delay

Fig. 7, presents the comparison of Overhead while varying the speed from 20 to 100 ms. It is clearly shown that the overhead of RMR is lower than LTDMS and HDTMP.

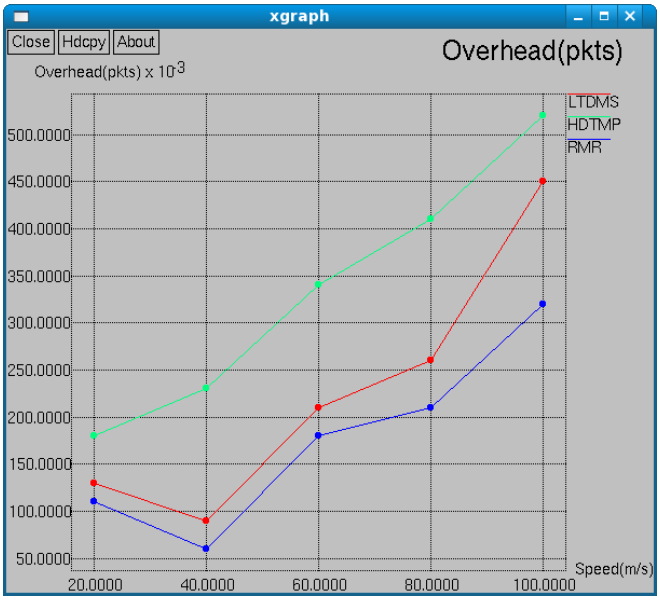

Fig. 7.Speed Vs Overhead

V. CONCLUSION

In WSNs, the best route is being determined by choosing efficient strategy to forward the data to the base station. Due to that, the node consumes more energy unnecessarily. In this paper, we have developed a reliable multicast routing scheme which attains cluster routing, multicast establishment, and determination of energy consumption to make balance between packet integrity, energy consumption and node lifetime to the sensor nodes. In the first two phases of the scheme, cluster routing and multicast route establishment are combined to achieve load balancing, minimum energy consumption and avoid network congestion. In third phase, minimum energy consumption model is proposed to achieve stable routing with minimum energy resources. It uses following factors, energy spent per packet during both transmission and reception to favor packet forwarding by maintaining high residual energy consumption for each node. We have demonstrated the energy consumption estimation of each node. By simulation results we have shown that the RMR achieves better performance than existing schemes.

REFERENCES

1. Lu Su, Bolin Ding, Yong Yang, Tarek F. Abdelzaher, Guohong Cao and Jennifer C. Hou, “oCast: Optimal Multicast Routing Protocol for Wireless Sensor Networks”, National Science Foundation under grant, 2009, pp.1-10.
2. K Ashok Babu, D Sreenivasa Rao and S. Lakshminarayana, “ Swarm Intelligence based Energy Efficient Routing Protocol for Wireless Ad-hoc Networks”, International Journal of Computer Applications, Vol.62, No.2, 2013, pp.34-39.
3. LeiWang, Yuwang Yang,Wei Zhao, Lei Xu, and Shaohua Lan, “Network-Coding-Based Energy-Efficient Data Fusion and Transmission for Wireless

Sensor Networks with Heterogeneous Receivers", International Journal of Distributed Sensor Networks, 2014, pp.1-13.

4. Zhi-jie Han, Ru-chuan Wang and Fu Xiao, "A Multicast Algorithm for Wireless Sensor Networks Based on Network Coding", International Journal of Distributed Sensor Networks, 2014, pp.1-9.
5. Mohan Kumar S, Thenmozhi R, Inian Lourde Alex A and Malarvizhi M, "A Hybrid Trust Based Secure Model for Wireless Sensor Network", International Journal of Emerging Trends & Technology in Computer Science, Vol.3, Issue 1, 2014, pp.144-147.
6. Fengjun Shang and Yang Lei, An Energy-Balanced Clustering Routing Algorithm for Wireless Sensor Network", Wireless Sensor Network, 2010, Vol.2, pp.777-783.
7. Mohsen Nejadkheirallah, " Multi-hop Fuzzy Routing for Wireless Sensor Network with Mobile Sink", Journal of mathematics and computer science, Vol.9, 2014, pp.12-24.
8. Stefanos A. Nikolidakis, Dionisis Kandris, Dimitrios D. Vergados and Christos Douligeris, "Energy Efficient Routing in Wireless Sensor Networks Through Balanced Clustering ", Algorithms, Vol.6, 2013, pp.29-42.
9. Kyuhong Lee and Heesang Lee, "Energy-Efficient Self-Organized Clustering with Splitting and Merging for Wireless Sensor Networks", International Journal of Distributed Sensor Networks, 2013, pp.1-12.
10. Min Yoon, Yong-Ki Kim and Jae-woo Chang, "An Energy-efficient Routing Protocol using Message Success Rate in Wireless Sensor Networks", Journal of convergence, Vol.4, No.1, 2013, pp.15- 22.
11. Mohammad S. Obaidat, Sanjay K. Dhurandher, Deepank Gupta, Nidhi Gupta and Anupriya Asthana, "DEESR: Dynamic Energy Efficient and Secure Routing Protocol for Wireless Sensor Networks in Urban Environments", Journal of Information Processing Systems, Vol.6, No.3, 2010, pp.269-294.
12. P.Sivaranjanadevi, and T.Poongothai, "Energy Efficient Routing and Fault Node Replacement Algorithm for Wireless Sensor Networks", International Journal of Communications Networking System, Vol.2, 2013, pp.183-187.
13. Xiao-Hui Li and Zhi-Hong Gua, "Energy-Aware Routing in Wireless Sensor Networks Using Local Betweenness Centrality", International Journal of Distributed Sensor Networks, 2013, pp.1-10.
14. Kyuhong Lee and Heesang Lee, "Energy-Efficient Self-Organized Clustering with Splitting and Merging for Wireless Sensor Networks", International Journal of Distributed Sensor Networks, 2013, pp.1-12.
15. Hamid reza Hassaniasl, Amir masoud Rahmani, Mashaallah Abbasi Dezfuli and Arash Nasiri Eghbali, "A Novel Score-Aware Routing Algorithm in Wireless Sensor Networks", International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (5), pp.397 – 404.
16. Yuxin Mao and Guiyi Wei, "A Feedback-Based Secure Path Approach for Wireless Sensor Network Data Collection", Sensors, 2010, Vol.10, pp.9529-9540.
17. K. Vanaja and R. Umarani, "An Adaptive Fault Tolerant Multipath Routing (AFTMR) Protocol for Wireless Ad Hoc Networks", European Journal of Scientific Research, ISSN 1450-216X Vol.79 No.2 2012, pp.180-190.