International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.4, No.6, June 2015 DOI:10.15693/ijaist/2015.v4i6.158-163

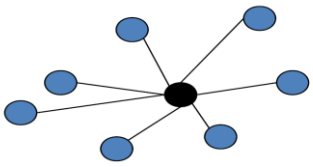
Using Residual Energy for Efficient Dynamic Source Routing in Wireless Ad Hoc Networks

B.Hemalatha[1], D.Venkatesh[2], K. Sai Priyanka[3]
[1]M.Tech Student, Dept of CSE, GATES Institute of Technology, Andhra Pradesh, India,
[2]Associate Professor in CSE, GATES Institute of Technology, Andhra Pradesh, India,
3Assistant Professor in CSE, GATES Institute of Technology, Andhra Pradesh, India,

Abstract: Energy efficient routing is an efficient mechanism for minimizing energy cost of data communication in wireless Ad Hoc networks. Normally, routes are revealed taking into consideration the energy consumed for E2E (end-to-end) packet traversal. However, this must not result in discovery of less dependable routes in the network. Energy-efficient routing in Ad Hoc networks is neither full nor well-organized without the concern of residual energy of nodes and reliability of links. Finding consistent routes can improve quality of the service. But, taking into consideration the residual energy of nodes in routing can keep away nodes from being overused and can finally lead to an increase in the operational life span of the network. The main objective of this paper is to propose an E-E-DSR (energy efficient dynamic source routing) protocol in mobile Ad Hoc networks (MANETs) to enhance the network life time. E-E-DSR is used as the base model due to the fact that it is a typical on demand protocol with less bandwidth and energy use. The existing energy efficient routing algorithms namely RMER (reliable minimum energy routing) and RMECR (reliable minimum energy cost routing) are enhanced and implemented in E-DSR.

I.INTRODUCTION

A WSN typically consists of two device types [2]. The first type is sensor nodes, also known as motes. The second is the base station, or gateway, or sink, which collects all data from the sensor nodes and stores it for later use. Each sensor node performs the main tasks, such as event detection, local processing and reporting to the base station. Some sensor nodes may fail due to a lack of power, or have physical damage or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network. Therefore, it is necessary to use a lot of nodes to obtain a reliable system. Two common topologies in WSNs are star and mesh. For



a star topology or single-hop WSN, all sensor nodes can communicate with the base station directly as shown in Figure 1.

Figure 1: Star Topology (Single-hop Network)

This topology is simple and does not require a routing protocol or extra overhead in the messages. However, this network has a limited coverage area which restricts applications to follow the range of radio communication.

The mesh topology covers a wide area by forming a multihop network. If the nodes are not within the transmission range of the base station, their messages have to be forwarded by other nodes as in Figure 2. The mesh topology requires an efficient and light Ad Hoc routing protocol.

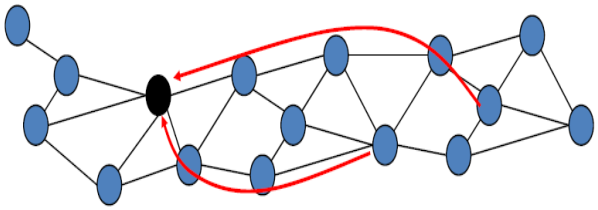


Figure 2: Mesh Topology (Multihop Network)

The role of relay nodes is very important, particularly the neighbours of the base stations. These nodes will consume more energy than others because they have to transmit their own data as well as forwarding data from others. In some cases, many sensor nodes may be unable to communicate with the base stations owing to the low energy of the relay nodes. In order to design

WSNs to provide some services that are needed, it is necessary to study the difference between the WSNs and other wireless networks. A WSN is similar to a Mobile wireless Ad-hoc Network (MANET) [3]. Both are composed of wireless devices that can dynamically self-organize to form a network without necessarily using any pre-existing infrastructure.

However, there are some differences between WSN and MANET. First, a MANET is usually a distributed network, while a WSN is a centralized system. A MANET device will normally open a communication channel with other devices in the network as part of its normal functionality. On the other hand, normal traffic in a WSN is sent from a sensor node to the base station. Second, many sensors may generate the same data within the phenomenon concerned. Such redundancy needs to be exploited to improve energy and bandwidth utilization. Third, unlike a node in a MANET, a sensor node usually has limited battery power, computation and memory capacity, which requires careful resource management. Finally, a MANET topology may change rapidly and unpredictably because it is a dynamic network with devices continuously entering and leaving the group. But in the case of WSN, all nodes usually stay inside the network.

II. RELATED WORK

Routing in Ad Hoc networks is, generally, multihop since units may not be within wireless transmission range of one another. Also routes can often get disconnected as units can move freely and randomly. Thus, routing protocols for Ad Hoc networks should be distributed and must adapt to frequent changing on the network topology, while keeping the communication overhead to a minimum. Routing protocols can be classified in:

Proactive routing protocols [4] these protocols attempt to maintain consistent and up-to-date routing information from each unit to every unit in the network. When a unit wants to send a message, the route to the destination is already known and can be used immediately. However, proactive routing protocols suffer the disadvantage of additional control traffic that is needed to continually update stale route entries.

Reactive routing protocols [5, 6] these protocols do not maintain information about all routes. Often, when a unit wants to send a message, it needs to find a route to the destination, and then it uses this route to send the message. Although reactive protocols need some time to find routes, they do not have the overhead of keeping up-to-date information about the entire network.

Hybrid routing protocols [7] these protocols mix the proactive and the reactive approaches, normally using a proactive approach inside a cluster or a zone of the network, and a reactive approach to an inter-cluster or an inter-zone communication.

Geographical routing protocols [8] also called location-based routing protocols; these protocols use location information to decrease the overhead of route discovery and/or route maintenance. The location information may be obtained using the GPS (Global Positioning System), or any other technique that allows the units to have some location information.

Power aware routing protocols [9] as the energy consumption of the network interface can be significant; a unit could save a considerable amount of power by turning it off. In Ad Hoc networks, however, units must participate of higher-level routing protocols and must cooperate with each other to deliver messages; consequently, a unit cannot simply turn off its network interface when it does not have anything to transmit. A good power saving coordination technique should have the following characteristics:

- It should allow as many units as possible to turn their network interface off most of the time, since even idle devices consume almost as much energy as active ones;
- It must forward messages between any pair of units as fast as if all units were awake. Thus, power saving and routing protocols must be coordinated [10].

Hierarchical routing protocols [11] hierarchical routing schemes are typically used by clustering protocols. The main idea of these protocols consists in grouping the units of the system into clusters in order to improve the scalability and/or to reduce the route acquisition delay. Normally these protocols implement a proactive routing strategy inside clusters, and a reactive routing strategy to route messages among clusters, thus reducing the overhead of the proactive protocols, and also reducing the delay of the route searching phase of the reactive ones.

Secure routing protocols [12] secure routing protocols are typically requested when the network is performing security-sensitive applications, like military tactical operations. Secure routing protocols should be

robust against dynamically changing topology and malicious attacks.

Quality of Service routing protocols [13] the provision of Quality of Service (QoS) relies on resource reservation. Hence, the data messages of a QoS connection are likely to flow along the same route, on which the required resources are reserved, the goal of QoS routing is two-fold:

- selecting routes that have sufficient resources to meet the QoS requirements of all admitted connections;
- Achieving global efficiency in resource utilization.

III. PROPOSED ROUTING ALGORITHM

Source routing is a routing technique in which the sender of a message determines the complete sequence of units through which the message should be forwarded. The sender explicitly lists this route in the messages' header, thus when unit i receives a message; it just looks in the header of the message and forwards the message to the next hop. Source routing has been used in a number of contexts for routing in wired networks, using either statically configured routes or dynamically constructed source routes.

The Energy aware Dynamic Source Routing (E-DSR) protocol [14] is an on-demand routing protocol that is based on the concept of source routing. Mobile units are required to maintain route caches, which contain the source routes of which the mobile is aware. Entries in the route cache are continually updated as new routes are learned. To send a message, the sender constructs a source route in the message's header, giving the address of each host through which the message should be forwarded in order to reach the destination. The sender then transmits the message to the first hop in the source route. When a unit receives a message, if the unit is not the final destination of the message, it simply transmits the message to the next hop in the source route of the message's header. When the message reaches its destination, it is delivered to the proper application.

As messages carry on the entire route between the source and the destination, other units forwarding this message or overhearing it can easily cache the routing information carried by this message.

In E-DSR, each unit maintains a route cache in which it keeps the routes that it has learned, i.e., a routing table that contains the discovered routes from the unit to the others. When a unit wants to send a message to another unit, it first checks its route caches for a route to the destination. If a route is found, it uses this route to transmit the message. Otherwise, the sender may attempt to discover a route to the destination, using the route discovery phase of the protocol. Each entry in the route cache has associated an expiration period with it, after which the route is deleted from the route cache.

A unit must monitor that a route stays connected while it is using it. In E-DSR this monitoring of the routes in use is called route maintenance. When route maintenance detects problems in a route, or receives a route error, the route discovery can be used again to discover a new and correct route to the destination.

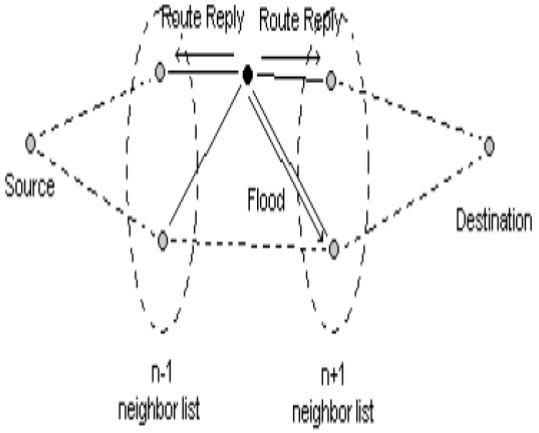


Figure 3: Proposed E-DSR Flow

3.1 Route Discovery:

Route Discovery allows any source to communicate with another mobile unit when the source has no route from itself to the destination in its route cache. To discover a route, a unit broadcasts a route request (RREQ), message. If the route discovery is successful, the sender of the RREQ receives a route reply (RREP), message with the sequence of hops through which it can reach the destination. A RREQ message contains: the sender's address, the destination's address, a unique request id and a route record. The sender and the destination addresses are the addresses of the respective units. The request id is set by the sender of the RREQ, to allow the other units in the network to detect duplicate received RREQ. The route record stores the request's history, in terms of hops, from the unit initiating the route, up to the unit that has just been reached by this RREQ. When a unit receives a RREQ message, it processes this message in the following order:

- If the pair (sender's address, request id) of this message matches a pair in this unit's list of recently received requests, then it discards the RREQ;
- Else, if this unit is the destination of this RREQ, then the route record of this message contains a route from the source to the destination. Thus, this unit returns a copy of this route to the sender of the RREQ in a RREP message.
- Else, this unit appends its own address to the route record and rebroadcasts the request.

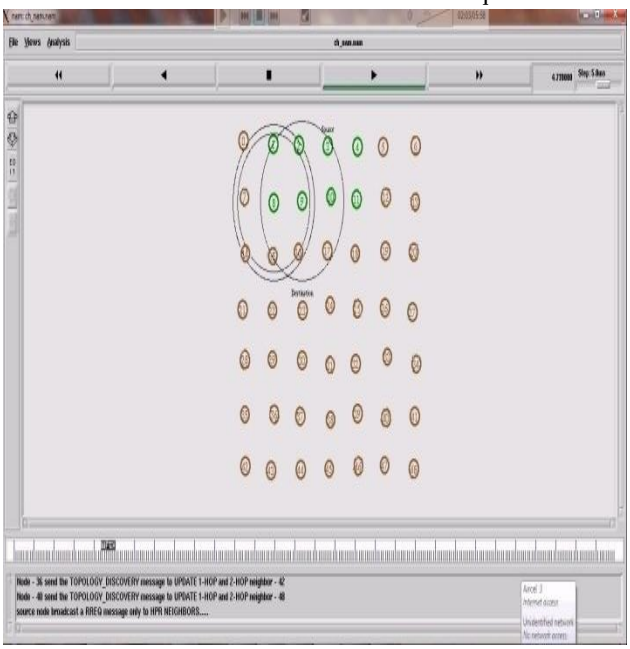


Figure 4: RREQ Process

The first step ensures that routes are loop-free, and removes later copies of the RREQ that can arrive to a unit through a different route. The two other steps ensure that the message is forwarded until it reaches the destination. Once the destination, unit j, receives a RREQ message, it reverses the route in the route record from the RREQ message, thus obtaining a route between itself and the sender of the RREQ, unit i. Then it sends a RREP message to unit i through the reverse route. When the RREP reaches unit i, a route is set up between units i and j.

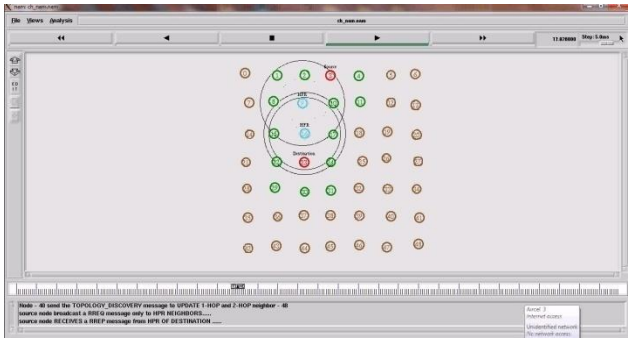


Figure 5: RREP Process

3.2 Route Maintenance:

When forwarding a message using source route, each unit transmitting the message is responsible for confirming that the message has been received by the next hop. In particular, E-DSR can use the so called passive acknowledgements: a unit hears the transmission of one of its neighbours to the next unit in the route. A unit can also perform route maintenance by setting a bit in the message to request an explicit acknowledgement from the next hop. If the transmission reports a problem that cannot be recovered, this unit sends a route error (RERR), message to the original sender of the message that encountered the broken link.

The RERR message contains the addresses of the units at both ends of the hop error, i.e., the unit that detected the broken link, and the unit to which it was attempting to send the message. The RERR message is forwarded through the reverse route of the message that encountered the broken link. When a unit receives a RERR message, it removes from its cache the route to the unit that causes the broken link, and also all routes that contain this unit. When the RERR reaches its destination, this unit decides if this route is still desired. If so, the route discovery is invoked again, to find another route.

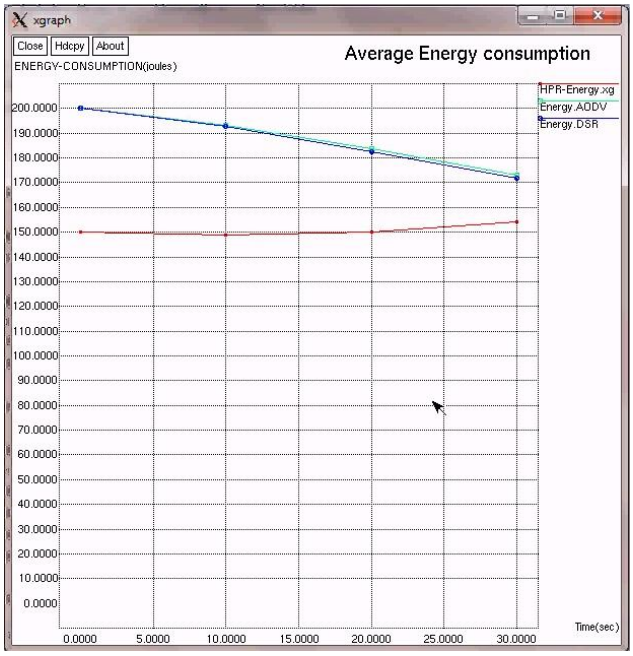
IV. EXPERIMENTAL RESULTS

The total validation of the proposed technique is done in NS2.35 environment and the simulation results are depicted below.

The results include the following metrics:

- Average Energy consumption
- Packet Delivery Ratio
- Packet Drop
- Throughput

The proposed method is indicated as HPR (high precision routing) indicated in red line and for comparison



this paper considered the traditional E-DSR (blue line) and AODV (Ad Hoc On Demand Distance Vector) routing protocol (green line).

Figure 6: Average Energy Consumption

The above figure (figure 6) shows that the energy consumed by the proposed EE-DSR is low when compared to the other existing protocols.

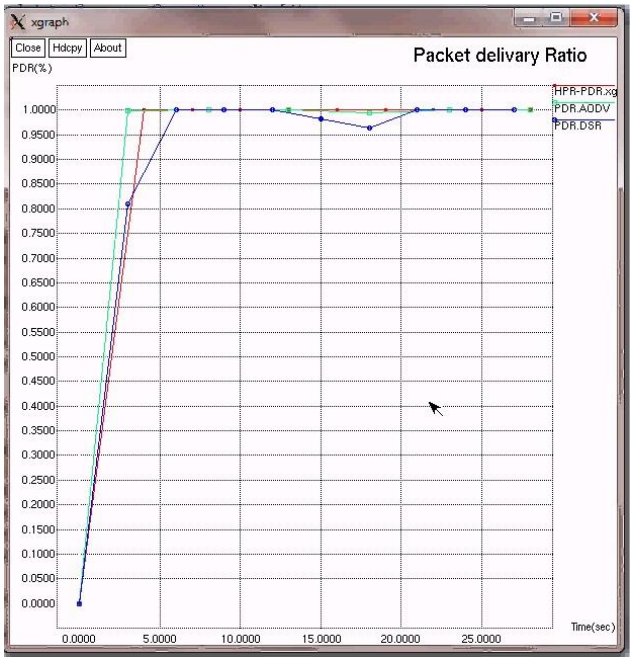


Figure 7: Packet Delivery Ratio

The figure 7 shows that the performance of all the three techniques in this regard is close to each other.

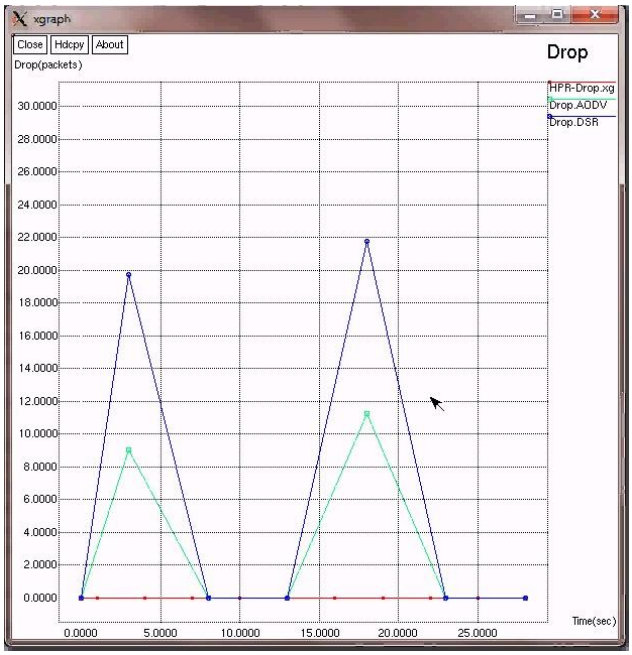
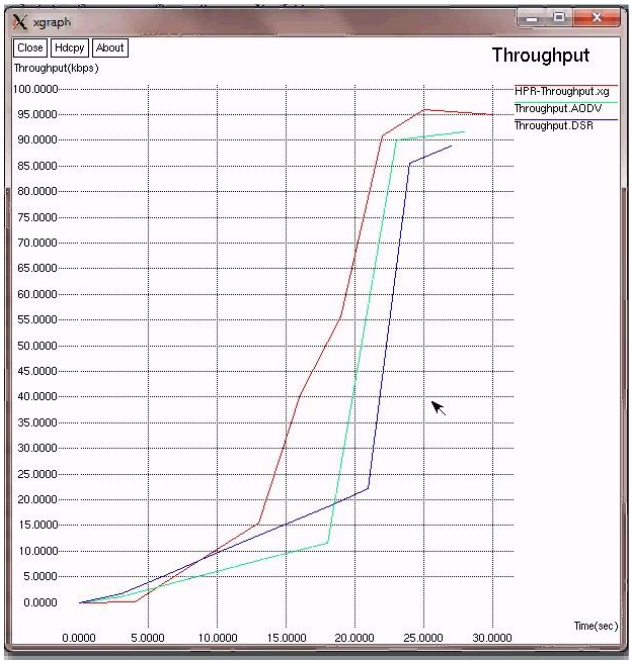


Figure 8: Packet Drop

Figure 8 shows that the packet drop ratio is



really low compared to the other existing schemes.

Figure 9: Throughput

The very important aspect of any routing is the throughput. The results of figure 9 demonstrate that

throughput is comparatively high when compared to the other existing schemes.

V.CONCLUSION:

This paper addressed an important research issue regarding routing in WSNs which is the energy efficient reliable routing namely an Energy aware Dynamic Source Routing (EE-DSR) algorithm for efficient data transmission. The EE-DSR consumes less energy and also promises a secure routing by selecting high efficient energy nodes as intermediate nodes. Further the high energy nodes are only used for data transmission and the low energy nodes are left over. The EE-DSR is tested and the analysis and results depict promising performance improvements.

REFERENCES:

[1] Javad Vazifehdan, R. Venkatesha Prasad, and Ignas Niemegeers, "Energy-Efficient Reliable Routing Considering Residual Energy in Wireless Ad Hoc Networks", IEEE Transactions On Mobile Computing, VOL. 13, NO. 2, February 2014, pp.434-447.

[2] Jun Zheng and Abbas Jamalipour. Wireless Sensor Networks: A Networking Perspective. Wiley-IEEE Press, 2009.

[3] Tracy Camp, Je_ Boleng, and Vanessa Davies. A survey of mobility models for AdHoc network research. Wireless Communications & Mobil Computing (WCMC): Special Issue on Mobile AdHoc Networking: Research, Trends and Applications, 2:483{502, 2002.

[4] T.W. Chen, and M. Gerla, "Global State Routing: A New Routing Scheme for Ad-hoc Wireless Networks," Proc. of the IEEE International Conference on Communications (ICC 2008), pp. 171-175, 2008.

[5] S. Agarwal, A. Ahuja, J.P. Singh, and R. Shorey, "Route-Lifetime Assessment Based Routing (RABR) Protocol for Mobile Ad-Hoc Networks," Proc. IEEE International Conference on Communications (ICC 2000), pp. 1697-1701, 2000.

[6] G. Aggelou, and R. Tafazolli, "RDMAR: A Bandwidth-Efficient Routing Protocol for Mobile AdHoc Networks," Proc. ACM International Workshop on Wireless Mobile Multimedia (WoWMoM 1999), pp. 26-33, 1999.

[7] Z.J. Haas, and M.R. Pearlman, "The Performance of Query Control Schemes for the Zone Routing Protocol," IEEE/ACM Transactions on Networking, vol. 09, no. 4, pp. 427-438, 2001.

[8] S. Basagni, I. Chlamtac, V.R. Syrotiuk, and B.A. Woodward, "A Distance Routing Effect Algorithm for Mobility (DREAM)," Proc. ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2008), pp. 76-84, 2008.

[9] L. Anderegg, and S. Eidenbenz, "Ad hoc-VCG: A Truthful and Cost-Efficient Routing Protocol for Mobile AdHoc Networks with Selfish Agents," Proc. ACM International Conference on Mobile Computing and Networking (Mobi-Com 2003), pp. 245-259, 2003.

[10] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "Span: An Energy-Efficient Coordination Algorithm for Topology Maintenance in AdHoc Wireless Networks," Proc. ACM International Conference on Mobile Computing and Networking (MobiCom 2001), pp. 85-96, 2001.

[11] Ephremides, J.E. Wieselthier, and D.J. Baker, "A Design Concept for Reliable Mobile Radio Networks with Frequency Hopping Signalling," Proc. IEEE,, vol. 75, no. 1, pp. 56-73, 2007.

[12] Y.C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for AdHoc Networks," Proc. ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2002), pp. 12-23, 2002.

[13] S. Chen, and K. Nahrstedt, "Distributed Quality-of-Service Routing in Ad-Hoc Networks," IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1-19, 2009.

[14] D.B. Johnson, and D.A. Maltz, "Dynamic Source Routing in AdHoc Wireless Netwoks," Mobile Computing - Chapter 5, Kluwer Academic Press, pp. 153-181, 2006.