

## Realization of Fault Tolerant Routing Protocol for Zigbee

<sup>1</sup>Sharmila Sankar and <sup>2</sup>Sankaranarayanan  
Department of Computer Science and Engineering,  
School of Computer and Information Science,  
B S A Crescent Engineering College, Chennai, India

---

**Abstract: Problem statement:** Increased use of handheld devices and sensor devices pose problems in existing routing protocols. The performance of the existing routing protocols deteriorates very much on these dense scenarios. Control overheads are very important parameter in deciding the performance of routing protocols, which are introduced during route discovery and maintenance process. Denser the network, higher is the control overhead in establishing and maintaining the communication path between end systems. This study aims at implementing an improved fault tolerant routing algorithm that minimizes the routing overhead for ad hoc networks using Zigbee. **Approach:** We propose a routing protocol which minimizes the routing overhead by exploiting the network density. The number of nodes involved in handling the control packets is minimized in the proposed protocol by selecting few of the neighbors of each node based on the received signal strength. The link breaks are maintained locally, thus by reducing the number of control overheads in the network. **Results:** The performance of the proposed protocol is tested using OMNet++ simulator. The implementation using Zigbee nodes indicate that the control overhead is reduced up to 80% in dense environments and 60% in heterogeneous and sparse thereby saving energy in the sensor nodes. **Conclusion:** The proposed protocol increases the energy conservation and hence the nodes life time and networks' lifetime.

**Key words:** Received signal strength, control overheads, local repair, zigbee

---

### INTRODUCTION

Mobile Ad-hoc Networks (MANETs) advocate self-configuration and adaptation of wireless links between communication devices (mobile nodes) that operate autonomously or as an extension to a wired infrastructure. The wireless communication links that form the network have to be characterized by a dynamic topology with no fixed infrastructure since the nodes are highly mobile. The nodes are equipped with antennas for reception and transmission within the communication medium through broadcasting. These nodes within MANETs have salient properties including limited power, relatively short communication distance, low processing power and limited bandwidth. Due to the highly dynamic nature of mobile nodes and the absence of a central controller, traditional routing protocols used for a wired network cannot be applied directly to a MANET. Some of the considerations required in the design of MANET routing protocols include the mobility of nodes, unstable channel states and resource constraints such as

power and bandwidth. In a MANET, the movement of nodes will cause communication between nodes to be disrupted due to frequent path breaks and reconnections. Also, the broadcasting of radio channels can be highly unstable and the network layer has to interact with the MAC layer for available channels. In addition, power availability is often limited since the nodes are connected to batteries. Currently, the network and upper layers of IEEE 802.15.4 is being implemented by the Zigbee Alliance. Details of Zigbee Routing protocols is discussed. It is worth pointing out that the main research efforts have focused on how to reduce the control packets in the network and hence increase the node lifetime with respect to limited battery energy. However, when real-time applications are deployed on them, extending the lifetime of the network should be done without jeopardizing real-time communications from sensor nodes to other nodes or to data sinks. For example, a surveillance system needs to alert authorities of an intruder within a few seconds of detection (Vicaire *et al.*, 2006).

---

**Corresponding Author:** Sharmila Sankar, Department of Computer Science and Engineering B S A Crescent Engineering College, Chennai, India

For energy saving, most of work focuses on the communication protocol design since in a WSN the radio communication unit is the major power consumer in the node (it consumes about one thousand CPU units) (Ergen and Varaiya, 2006). IEEE 802.15.4 Task Group together with Zigbee Alliance has developed an entire communication protocol stack for Low-Rate Personal Area Networks. One of the potential applications of this standard is in WSNs. This standard 2 represents the new generation of distributed embedded systems for pervasive computing. IEEE 802.15.4 standard deals with the energy optimization in the physical layer and the Medium Access Control (MAC) sub-layer. Energy saving is mainly achieved by defining a sleeping period (inactive period) in a super frame. The Zigbee specifications define the routing and the application layer. The Zigbee routing protocol is almost the same as Ad hoc On Demand Distance Vector (AODV) with the exception of route maintenance. AODV always choose the route that minimizes the delay (or equivalently the number of hops), but it does not take into account energy optimization. In this study, we aim at improving the Zigbee routing protocol by including both energy and delay considerations. Several energy-aware metrics have been proposed (Busse *et al.*, 2006; 2007) to optimize the energy consumption during the routing process. However, it does not take into account the path's reliability and the impact of link breaks, which may occur frequently due to the mobility of nodes. It should be noted that it causes higher retransmissions, which in turn increase the energy consumption and longer delay. In this study, we will focus on minimizing the energy consumption by reducing the number of nodes handling the RREQ packets and delay in path re-establishment by proactive link repair mechanism. Our main idea is to realize the improved fault tolerant AODV protocol, which was tested using simulators. In our study, we used IEEE 802.15.4 protocol and Zigbee AODV. We minimize the energy consumption and the delay at the routing layer.

#### **Routing protocols:**

**Zigbee routing protocols:** The MAC and PHY layers of IEEE 802.15.4 have no notion of node resources and energy. At the network layer, Zigbee supports node activation, network discovery, network formation and routing of packets. Similar to IEEE 802.15.4, Zigbee is an industrial standard that is targeted for low data rate, low power consumption, low cost as well as long life wireless network operations. Zigbee employs a basic master-slave configuration where each master can

support up to 254 slaves that can be nested to support a hierarchical routing strategy (Hoffert *et al.*, 2005). In addition, Zigbee provides a unique feature of redundancy in communication hence eliminating single point of failure in mesh networks. The routing algorithms defined for use by Zigbee are the Ad Hoc On Demand Distance Vector (AODV) protocol and the Cluster Tree protocol. We propose an enhancement to AODV protocol to minimize the control packets in the network and thus reduce the energy consumption and minimize the delay.

#### **Ad Hoc on Demand Distance Vector (AODV)**

**protocol:** The AODV is a pure on-demand acquisition algorithm system that allows message passing to nodes that are unreachable through neighboring nodes (Perkins and Royer, 1999). Routing is accomplished by discovering the shortest possible route and ensuring that these routes do not contain loops. AODV also has the ability to adapt to route changes and can create new routes when error occurs. Individual mobile nodes operate as a special router where routes are obtained only when required with minimal reliance on periodic updates. Nodes not within the active paths neither maintain any routing information nor participate in exchanging routing tables. However, a route needs to be discovered or maintained when there is communication between two nodes or that the nodes are in the direct path between the source and destination nodes. In essence, the improved fault tolerant AODV seeks to minimize the number of control messages flowing in the network.

#### **Proposed protocol:**

**Route discovery:** Our scheme builds routes on demand via a query and reply procedure. When a source needs to initiate a data session to a destination but does not have any route information, it searches a route by selective border node retransmission technique (Sankar, Sankaranarayanan, 2010). Each Route Request (RREQ) packet has a unique identifier so that nodes can detect and drop duplicate packets. An intermediate node, upon receiving a non-duplicate RREQ, records the previous hop and the source node information in its route table. It then multicasts the packet or sends back a Route Reply (RREP) packet to the source if it has a route to the destination. The destination node sends a RREP via the selected route when it receives the first RREQ. To reduce the number of control packets generated only the farthest nodes are allowed to rebroadcast the RREQ packets (Fig. 1).

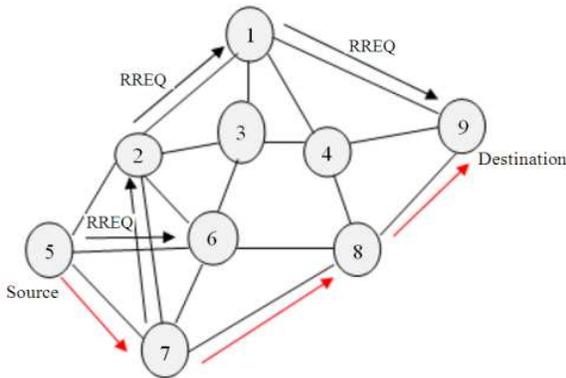


Fig. 1: Route discovery

Every node that rebroadcasts the RREQ makes an entry in its routing table and waits for the reply from the destination to arrive before the timer expires. If the RREP is not received before timer expires, then partial entry made in the routing table is purged else if the node receives the reply then the successor node in the path to the destination is recorded in the routing table. The intermediate nodes that relay the RREP packet become forwarding nodes. The following is the algorithm for setting up a path between source and the destination node.

//Sending RREQ: Route Request will be sent by the source node if no route exists between the source and the destination nodes.

```

If (no route exists)
{
    Choose the few border nodes//determined by
    reachability parameter
    Create a RREQ packet
    Add (dest addr, broadcast ID,) to route table
    Locally broadcast RREQ setting up wait time for
    RREP
}

```

//Receiving RREQ: When a node receives a RREQ packet, it checks whether it is the intended destination. If so it sends the RREP packet else rebroadcasts the RREQ if it is one of candidate for rebroadcasting. If (you are the destination of RREQ || have fresh route to destination)

```

{
    Create a RREP packet;
    Unicast the RREP to the source of RREQ//using
    precursor list
} else if (candidate node for rebroadcasting)
{
    Choose the few border nodes;
    //determined by reachability parameter
    Modify RREQ packet; //add new border
    nodes for rebroadcasting
}

```

```

Create a route entry for source addr in
the route table;
Locally broadcast RREQ;
}

```

//When a node receives a RREP for the RREQ it forwarded then it makes an entry in routing table thus setting up the forward route and forwards the RREP to the source node.

If (destination seq. no. in RREP >= destination seq. no. in routing table)

```

{
    Update routing table;
    If (current node != source node) Forward the RREP;
    //using precursor list
}

```

**Route maintenance:** As the nodes in the network are mobile, the path established is not guaranteed to be intact till the entire communication session. Therefore the protocol should be aware of the nodes mobility during the data transmission session too and confirm that there are no link breaks due to nodes mobility in order to avoid link breaks (Banerjee and Dutta, 2010). AODV fix up the link breaks only after its occurrence, which leads to delay and packet drops. To overcome the delay incurred in finding the new path and avoid packet drops, our proposed protocol employs a proactive local error recovery technique. The technique employed in our proposed protocol is as follows:

- When a mobile node is likely to cause a link break, it intimates its predecessor node along the active path. A node senses its movement away from its successor node by checking the signal strength of the received packets. A mobile node is likely to cause link break when the received signal strength is very weak (threshold -90)
- Upon the reception of link error signal, the predecessor node broadcast link repair packets to its one hop neighbors with the address of the successor node of the node that is likely to cause link break, thus distinguishing between local connectivity management and general topology maintenance
- The neighboring mobile nodes that have the information about successor node replies and one of these reporting nodes is considered as a new intermediate node
- If the neighboring nodes have no link with the successor node, then the Path Discovery process is initiated

Figure 2 Route Recovery Fig. 3 Route re establishment Fig. 2 and 3 illustrate the route maintenance mechanism. One of the intermediate nodes, node 7 in the example, moves away from the active path and is likely to cause link break. This likelihood to create link break is sensed by the node by checking its received signal strength.

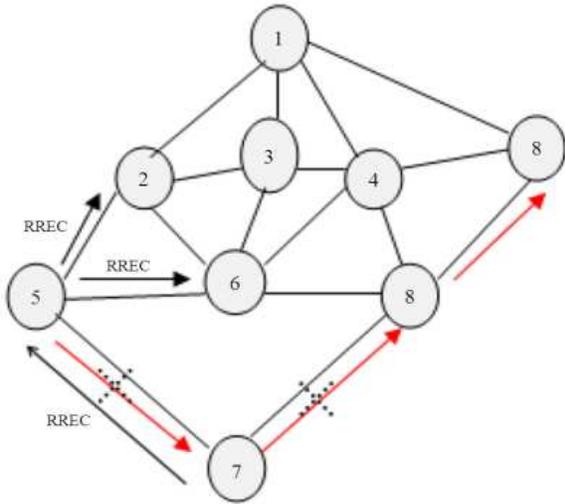


Fig. 2: Route recovery

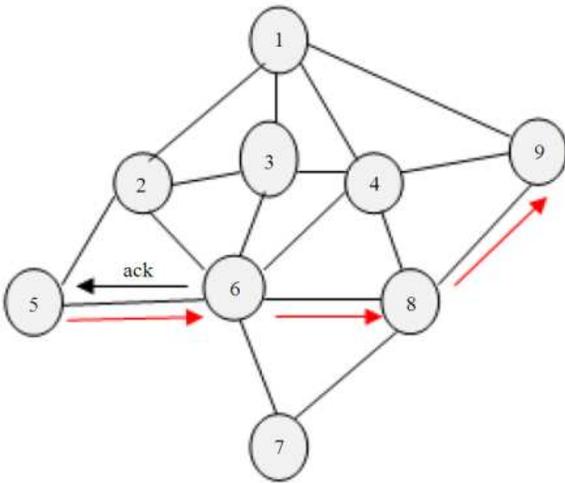


Fig. 3: Route re establishment

When the strength of the received signal goes beyond -90dbm, the node unicasts' a Route RePair (RRP) packet to its predecessor node in the active path. On reception of the RRP packet, the predecessor node identifies a new intermediate node to replace the node that is likely to create link break and patches the path. The predecessor node identifies a node that is a common neighbor of itself and successor of node this is likely to cause link break. In the case of dense network, the probability of finding such a node is very high.

**Data structures and packet headers:** Figure 4a shows the variation in header format of RREQ packet as compared with the RREQ packet format of AODV.

Type	HopCount	Src Seq. no	Src IP	Dest. Seq. no	Dest IP	RBnodelist
------	----------	-------------	--------	---------------	---------	------------

(a)

Type	HopCount	Src IP	Dest. Seq. no	Dest IP
------	----------	--------	---------------	---------

(b)

Type	HopCount	Successor
------	----------	-----------

(c)

Type	Predecessor	Successor
------	-------------	-----------

(d)

Fig. 4: Packet Format, (a) RREQ Packet (b) RREP Packet (c) RRP Packet (d) RREC Packet

Table 1: Route table

Src IP	Dest IP	PreCurList	NextHop	HopCount
--------	---------	------------	---------	----------

Table 2: Neighbor table

Neighbor IP	RSSI
-------------	------

RBnodelist field denotes the nodes chosen for rebroadcasting the RREQ packet and their IP addresses. The predecessor field is set to the address of node that rebroadcasts the RREQ. HopCount field in RREQ packet denotes the number of hops left to the packet to travel further in the network. This avoids routing loops in finding the path between the two end systems. The Fig. 4 b-d are the formats of route reply (RREP), Route Repair (RRP) and Route REcovery (RREC) packets respectively. The Type field denotes the packet type and the HopCount denotes the number of hop the packet had already traversed in the network. This gives the path length of the active path to be set up between the end systems. 5

The route table (Table 1) is maintained by all the nodes in the active path. The information in the route table enables the data packet to reach the destination node. The route table consists of the following information.

The following is the neighbor table shown in Table 2 is maintained by the nodes in the network. It consists of two fields namely the Neighbor IP, which stores the IP addresses of the neighboring nodes and the Received Signal Strength Indicator (RSSI) field stores the strength of the received signal of the respective nodes. The information in the neighbor table is used to choose the farthest or the border nodes for rebroadcasting the RREQ packets unlike AODV where all the neighboring nodes are involved in rebroadcasting the RREQ packets.



Fig. 5: A Zigbee network node displaying its neighbors addresses and RSSI

Start delimiter (Byte 1)	Length (Byte 2)	Length (Byte 3)	(Byte 4)	(Byte 5)	Frame data (Bytes 6-13)
7E	MSB	LSB	APLLD	Frame ID	64-Bit destination address
(Bytes 14-15)	(Byte 16)	(Byte 17)	(Byte(s) 18-n)	Checksum Last byte	
16-Bit destination network address	Broadcast radius	Options	RF data		

Fig. 6: Zigbee pro API frame format

**Test bed:** The protocol was testbed creating a test bed of 5 Zigbee nodes. Our primary design goal for the testbed was to test the protocol whether the number of control packets flowing in the network is reduced when the network is dense and the mobility condition is moderate. The Zigbee nodes in the network are configured in ad hoc mode and each of these nodes communicates 900 MHz radios, implementing IEEE 802.15.4 MAC protocol. All communications among the ad hoc network nodes is routed by the improved fault tolerant AODV protocol. AODV is a network layer routing protocol that operates at the IP layer of the network stack (OSI layer 3) and permits interoperation between different physical network interfaces. However, our protocol implementation conceptually operates as a virtual link layer just under the normal IP layer. This allows the protocol to route packets using IP addresses as flat identifiers when the other nodes in the ad hoc network are not organized as hierarchical subnets. Nodes in the network are assigned IP addresses

from a single subnet. Figure 5 shows a Zigbee node configured with the proposed routing protocol. The Zigbee mobile nodes are designed to display the IP address of the neighbor nodes and the absolute value of RSSI. It is also configured to display the previous and the next hop nodes addresses to check the path discovered for communicating between end systems.

The API's used to transmit and receive various packets is shown in Fig. 6. The RF Data field is used to exchange the information pertaining to the proposed protocol.

## CONCLUSION

The simulated conditions with OMNet++ for 802.11 protocols has been modified for Zigbee with AODV and various conditions has been tested to verify the working of the proposed protocol. The proposed protocol is also tested in a test bed consisting of 5 Zigbee nodes configured in ad hoc mode and it is seen that the number of route request rebroadcasts is reduced as expected. It is also seen that the link breaks due to the mobility of the nodes were handled locally thus reducing the control overheads in the network. This suggests that this kind of reduction in control overheads will lead to decrease in energy depletion and hence increase in the network life time in networks using Zigbee.

## REFERENCES

- Banerjee, A. and P. Dutta, 2010. Link stability and node energy conscious local route-repair scheme for mobile ad hoc networks. anuradha banerjee and paramartha dutta. Am. J. Applied Sci., 7: 1139-1147. DOI: 10.3844/ajassp.2010.1139.1147
- Busse, M., T. Haenselmann and W. Effelsberg, 2006. Poster-Abstract: A lifetime-efficient forwarding strategy for wireless sensor networks. University of Mannheim, Germany.
- Busse, M., T. Haenselmann and W. Effelsberg, 2007. Energy-efficient aggregation forwarding for wireless sensor networks. Proceedings of the International Conference on Sensor Technologies and Applications, Oct. 14-20, IEEE Xplore Press, Valencia, pp: 584-589. DOI: 10.1109/SENSORCOMM.2007.4394983
- Ergen, S.C. and P. Varaiya, 2006. PEDAMACS: Power efficient and delay aware medium access protocol for sensor networks. IEEE Trans. Mobile Comput., 5: 920-930. DOI: 10.1109/TMC.2006.100
- Hoffert, J., K. Klues and O. Orjih, 2005. Configuring the IEEE 802.15.4 MAC layer for single-sink wireless sensor network applications. Washington University in St. Louis.

- Perkins, C.E. and E.M. Royer, 1999. Ad-hoc on-demand distance vector routing. Proceedings of the 2nd IEEE Workshop Mobile Computer System and Applications, Feb. 25-26, IEEE Xplore Press, New Orleans, LA, USA., pp: 90-100. DOI: 10.1109/MCSA.1999.749281
- Sankar, S. and V. Sankaranarayanan, 2010. Framework for probabilistic routing in dense MANETs. Recent Trends Networks and Commun., Commun. Comput. Inform. Sci., 90: 447-456. DOI: 10.1007/978-3-642-14493-6\_46
- Vicaire, P.T.H., T. Vicaire, L. Yan, L. Luo and G. Gu *et al.*, 2006. Achieving real-time target tracking using wireless sensor networks. Proceedings of the 12th IEEE Real-Time and Embedded Technology and Applications Symposium, Apr. 4-7, IEEE Xplore Press, pp: 37-48. DOI: 10.1109/RTAS.2006.9