Comparison and Analysis of RREQ and RREP for Dynamic Wireless Network

Navjot Kaur[1]
Ambala Colloge of engineering, Ambala.
Navjot8saini@yahoo.in
Arun Singh[2]
NIT Jalandhar, Punjab.
Sam700007@gmail.com

Ashok kumar[3],
Ambala Colloge of Engineering, Ambala.
Ashokcalicut1993@gmail.com
Manju B Shrma[4]
DAVIET, Jalandhar
sharmamanjub@rediffmail.com

***Abstract*— This paper compares and analyzes RREQ and RREP for wireless networks using Zigbee technology for transferring data between dynamically moving nodes. The system is simulated on Ptolemy 2 Visual Sense simulating tool, using power loss channel for 2, 4, 6, 8 number of composites nodes, with three different scenarios of different ranges of 250, 300 and 450. Result compares RREQ and RREP for data packet generated and data packets received, in above conditions and contrast significant difference.**

Keywords—*Zigbee*, RREQ, RREP, AODV and Visual Sense.

I. Introduction

ZigBee technology is a low data rate, low power consumption, low cost; and remote control applications. And connectivity for equipment that needs battery life as long as several months to several years but does not require data transfer rates as high. The data rate is 250kbps at 2.4. ZigBee uses a basic master-slave configuration suited to static star networks of many infrequently used devices that small data packets.[1] Other design goals are also maintained in the proposed protocols. The existing routing protocol AODV supports three phases, Route Request (RREQ), Route Reply (RREP) and Packet Delivery. [2] Each node in a mesh network employing AODV contains a routing table, with entries to the different destination nodes it knows how to reach. A routing table entry is indexed by the destination address, and includes the address of the next hop in the path, the hop count to travel, a destination sequence number, a route neighbor list, and an expiration time. Should a node try to transmit data to another node that is not in its routing table, the node will attempt path discovery. Path discovery is performed by broadcasting a route request (RREQ) packet. The RREQ packet contains several namely source and destination addresses, source and destination sequence numbers, a broadcast ID, and a hop count. The source address and broadcast ID together uniquely identify a RREQ packet .Once the RREQ packet arrives at a node, the node that it has not received this particular RREQ packet; it drops the packet. It then checks its own routing table to see if it knows of a valid route to the destination. A route is valid if the routing table entry's destination sequence number is larger than the one present in the RREQ packet. If the routing table does not contain such a route, the node increments the hop count in the RREQ packet and rebroadcasts it. If a node does contain a valid route to the destination in its routing table, it unicasts a route reply (RREP) packet to the source node. Every node receiving the RREQ packet so far has kept in memory the address of the node that directly sent it the RREQ packet. This information is used to construct a reverse route back to the source for the RREP packet to follow. The RREP packet contains for source and destination addresses, destination sequence number, hop count, and lifetime. The source and destination correspond to the same source and destination of the RREQ packet. Each node that receives the RREP packet updates its routing table and retransmits the packet towards the source. If there is more than one node with a valid route, though, multiple RREP packets will be sent to nodes on the reverse path. To reduce bandwidth use without quality results, a node will only retransmit a RREP packet if the destination sequence number is greater than the one stored in its routing table. The source can act once it receives an RREP packet; meanwhile, nodes that received the RREQ packet but not the RREP packet will timeout, erasing their reverse path memory. [3]

2. SYSTEM DESCRIPITION

S first checks its route table to determine whether it already has a route to D. If such a route exists, it can use that route for packet delivery, otherwise route discovery is needed. Route discovery process consists of following processes. In this section we have discussed our two proposed algorithm, with the following set of symbols:

i. S = Source node, D = Destination node CN= Current node, RP = Reverse Parent IP, FP = Forward Parent IP

ii. IR =Intermediate Routers or nodes between S and D.

iii. RREQ = Route Request message, RREP = Route Reply.

iv. RREQ ID.s.id, RREQ ID.dis.id = Route Request id with corresponding extension.
(.s.id) S broadcasts first time for 1hop destination. (.dis.id) S broadcasts second time for multi hop destination to discover route.

RREP ID.s.id, RREP ID.dis.id = Route Reply id with corresponding extension.
(.s.id) It is for one-hop destination node. (.dis.id) It is for multi-hop destination node.

v. RT = Routing Table. vi. RREQ_RP = RREQ parameter: <S, D, hop count, sequence number, RP, RREQ ID>.

vii. TR = Transmission Range of a node

viii. Nack = Acknowledgment to ensure that destination has received the RREQ and to inform other non-transmitted nodes not to transmit further identical RREQ and discard it.

RREQ Process:

1. S broadcasts the RREQ of (RREQ ID.s.id) first. 1.a. If D is in the TR of S, then S sends the RREQ directly to the D.D returns RREP of unique ID (RREP.s.id) to the S, within (TRREQ.s+TRREP.s). Other 1hop nodes are not D and they check the extension part of the RREQ ID, if it is (.s.id) then they discard it.

1.b. Else If S does not receive RREP of unique ID (RREP.s.id) from D within (TRREQ.s+TRREP.s), then it broadcasts the RREQ of unique ID (RREQ.dis.id) to find the D. IR receive this and check the extension part of the RREQ ID , if it is (.dis.id) then they pass it until the D is found. IR and D store the RP, which is next hop to the S from CN (While forwarding RREQ, S does not need to store the RP) and also stores the RREQ ID.

All nodes maintain the RREQ_RP. All nodes which have already broad-casted RREQ once, discard identical RREQ till 2TRREQ.dis after broadcasting RREQ.

2. When D receives a RREQ of unique ID (RREQ.dis.id), it discards identical RREQ till 2TRREQ.dis.

After receiving first RREQ, D broadcasts Nack to stop unnecessary further broadcasting of identical RREQ. After receiving Nack other nodes, which have not broad-casted identical RREQ. All IR which have already broad-casted RREQ once, discard Nack of same ID.

RREP Process:

3. When D receives first RREQ, it initiates RREP.

3. a. If S is in the TR of D, then D sends the RREP of unique ID (RREP.s.id) directly to the S, within the time (TRREQ.s+TRREP.s).

3. b. Else D places the IP address of S, as well as its own IP address into the RREP of unique ID (RREP.dis.id) and then D sends it to its RP which is next hop to the S. The RP of D is now the CN. This CN places its own IP into the RREP of unique ID (RREP.dis.id) and then it will send the RREP to its RP. This procedure continues until the S is reached. In RREP process, no need to maintain any parent information. [3]

Packet Delivery:

4. It is done by unicast method. R sends the packet to its next hop node to the G. R deletes the RP from its RT. The next hop node to the G of R is now the wireless composite. This wireless composite send the packet to its next hop node to the G, which is next hop to the G. This procedure continues until the G is reached.

This is the simple version of protocol so that it simulation as a fast as possible. The modal has the main characteristics of Zigbee, but without separate
layer. This version just implements a very simple AD- Hoc on demand distance vector routing.

2.1 Link Visualizer:-

This actor implements the channel listener interface.it creates a lines b/w two communicating
Nodes that are within the range of one another.it register itself with the wireless channel.it notified the transmission occurs on the channel on which is listening.

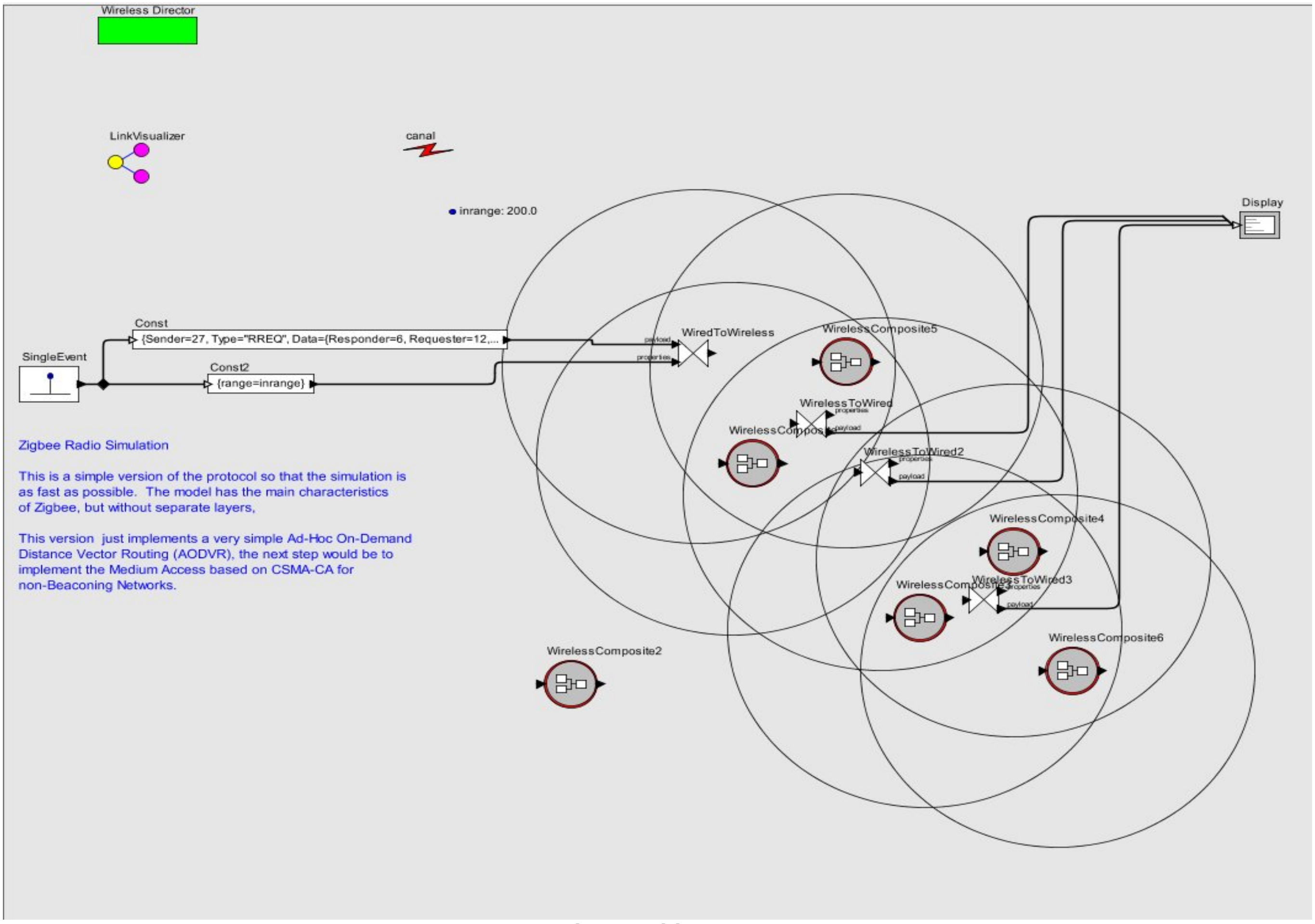

Fig.1 Simulation Model

2.2 Wireless Composite:-

It can composite actor for use in wireless domain.it creates instances of wireless IO port.

2.3 Wireless Director:-

Director for the Wireless model of computation. It creates instances of Wireless Receiver.

2.4 Single Event:-

This actor produces an event with the specified value. At the specified time.it queues an event. No event will be produced.

3. RESULTS

In this section, we present our experimental data in tabular and graphical forms, along with our interpretation of the data. For all the simulations, the same movement models were used, the number of traffic sources was fixed at different ranges250, 300,450 inrange. The maximum numbers of data packets are to be sending in number of wireless composite.

1. Packets delivery at range of 250: -

The on-demand of network AODV performed particularly well. The numbers of data packets are send RREQG which has data to be generated for the wireless composite. It has also generates the packet of wireless composite with the factor of increasing with a growing number of sources. [6] when the number of sources is low, the performance of AODV is similar regardless.

Table 1. Number of Data Packets at Range of 250

Number of Wireless Composite	**Number of Data Packet**			
	RREQR	**RREQG**	**RREPR**	**RREPG**
2	6	10	2	4
4	11	23	2	7
6	22	53	2	11
8	14	73	2	4

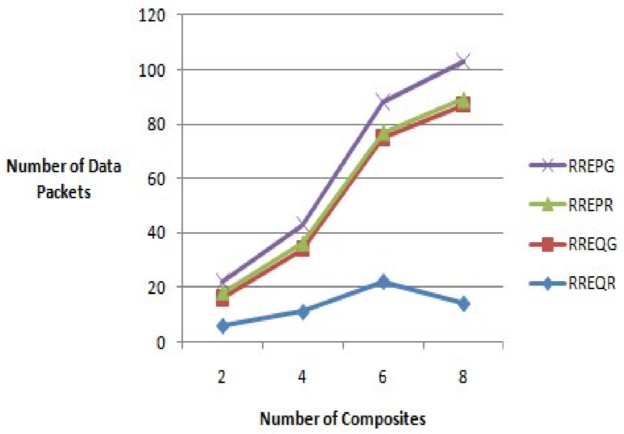

Fig3.1 At Range of 250

2. Packets delivery at range of 300:-

Table 2. Number of Data Packets at Range of 300

Number of Wireless Composite	Number of Data Packets			
	RREQR	RREQG	RREPR	RREPG
2	6	10	2	4
4	11	24	2	8
6	10	39	2	12
8	25	46	2	12

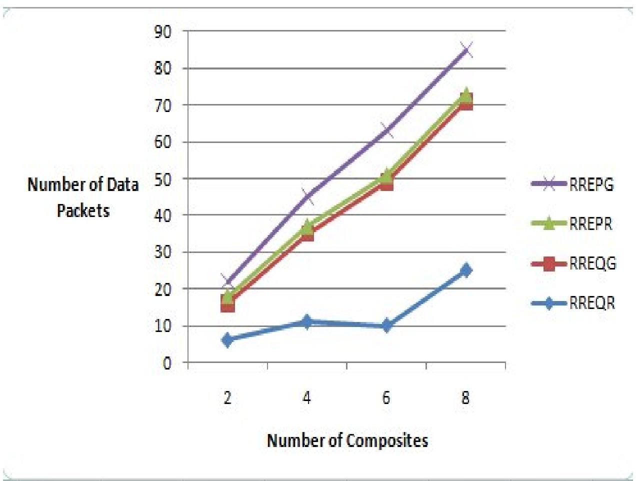

Fig3.2 At Range of 300

3. Packets delivery at range of 450:-

Table 3. Number of Data Packets at Range of 450

Number of Wireless Composite	Number of Data Packets			
	RREQR	RREQG	RREPR	RREPG
2	7	10	3	4
4	12	24	3	8
6	20	48	3	12
8	26	75	3	10

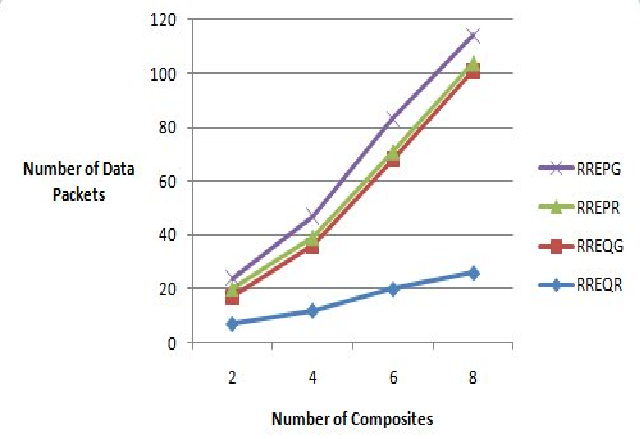

Fig3.3 At Range of 450

The major contribution to AODV routing over-head is from route requests, while route replies constitute a large fraction routing overhead. Furthermore, AODV has more route requests the converse is true for route replies. The simulation results bring out some important characteristic differences between the routing protocols. The different basic working mechanisms of these protocols leads to the differences in the performance.

4. CONCLUSION

This article puts forward a kind of differentiating study of RREQ and RREP for dynamic wireless network using Zigbee technology for data transmission. The data packets reached at destination is constant by using RREP in various ranges. Maximum data packets reached by using RREQ at range of 300 is 25 when generated is 46 for 8 number of composites.

5. References

[1] Sinem Coleri Ergen," ZigBee/IEEE 802.15.4 Summary,"Thesis.
[2] Swarnali Hazra University of Calcutta, India,
[3] Sanjit Setua University of Calcutta India,"Optimization on Control Overhead in MANET,"International Journal of Computer Applications (0975 – 8887).
[4] Chester Hamilton Texas A&M University, Varun Sampath University of Pennsylvania,"
[5] Performance of ZigBee PRO Mesh Networks
[6] with Moving Nodes,"IEEE.
[7] Sukhvinder S Bamber Department of Computer Science & Engg. National Institute of Technology Jalandhar, Punjab, India, Ajay K Sharma Department of Computer Science & Engg. National Institute of Technology
[8] Jalandhar, Punjab, India," Enhancing Network Output Load in IEEE 802.15.4with Different Modulations for Wireless Sensor Networks,"International Journal of Computer

[9] Applications (0975 – 8887).
[10] Deepti Gupta and Ajay K. Sharma Department of Computer Science and Engineering,National Institute of Technology, Jalandhar, Punjab, India,
[11] “On Routing Protocols for WSNs with Additional
[12] Layers: Future Technology for IT”,JOURNAL OF ADVANCES IN INFORMATION TECHNOLOGY.
[13] A.F.A. Abidin1, N.S.M. Usop2 and M.K. Yusof3
[14] Faculty of Informatics, Universiti Sultan Zainal Abidin, Kuala Terengganu, Malaysia,”Performance Comparison of Wireless
[15] Ad Hoc Routing Protocols,” International Journal.
[16] Taehong Kim, Daeyoung Kim, Noseong Park*, Seong-eun Yoo, Tomás Sánchez López,”Shortcut Tree Routing in ZigBee Networks,”2007 IEEE.
[17] Pedram Radmand[1], Marc Domingo[2], Jaipal Singh[1], Joan Arnedo[2], Alex Talevski[2], Stig Petersen[3], Simon Carlsen4,”ZigBee/ZigBee PRO security assessment based on compromised cryptographic keys,”2010 International Conference on P2P.
[18] Hongwei Li, Zhongning Jia, Xiaofeng Xue,”
[19] Application and Analysis of ZigBee Security Services Specification,”2010Second International Conference on Networks Security.