International Journal of Advanced and Innovative Research (2278-844)/

Volume 7 Issue 11

Performance Evaluation of AODV Routing Protocol in Wireless Sensor Network under the Influence of Fault Nodes

Jyotsna Rathee[1], HarkeshSehrawat[2], Chitra Saini[3]

Department of Computer Science and Engineering,
University Institute of Engineering and Technology,
Rohtak, India
(jyotsnarathe@gmail.com)
(sehrawat_harkesh@yahoo.com)
(chitrasaini13@gmail.com)

***Abstract*: - There is a remarkable growth in the field of Information Communication Technology (ICT) in Developing Countries (DCs).Wireless Sensor Network is one of the areas where ICT is recording an ongoing rapid change. Typically, a wireless sensor node (or simply sensor node) consists of sensing, computing, communication, actuation, and power components. We apply our scheme to the Ad-hoc On-Demand Distance Vector (AODV) protocol and evaluate the performance by simulation. We have used Qualnet tool to analyze the performance of AODV protocol in WSN under the influence of various faults**

***Keywords:* - WSN, RREQ, RREP, Fault**

I. INTRODUCTION

Due to recent technological advances, the manufacturing of small and low-cost sensors has become technically and economically feasible.WSN is the collection of hundreds or thousands of tiny sensor nodes having the abilities of sensing, computations and communication among each other or with the base station. The functional architecture of sensor nodes consists of four units which are sensor, CPU, radio and power. Sensor is a tiny device used to sense the ambient condition of its surroundings, gather data, and process it to draw some meaningful information which can be used to recognize the phenomena around its environment. These sensors can be grouped together using mesh networking protocols to form a network communicating wirelessly using radio frequency channel. The collection of these homogenous or heterogeneous sensor nodes called wireless sensor network (WSN). Advantages and application domain of WSNs varies from environmental monitoring, to health care applications, military operation, to transportation, to security applications, to weather forecasting, to real time tracking and a lot more.

II. AD-HOC ON DEMAND DISTANCE VECTOR (AODV) PROTOCOL

AODV protocol is a routing protocol in a reactive routing protocol

- Uses bi-directional links
- Route discovery cycle used for route finding
- Maintenance of active routes
- Sequence numbers used for loop prevention and as route freshness criteria
- Provides unicast and multicast communication

AODV discovers routes as and when necessary. It does not maintain routes from every node to every other. Routes are maintained just as long as necessary. Every node maintains its monotonically increasing sequence number and increases every time the node notices change in the neighbourhood topology.

AODV utilizes routing tables to store routing information

- A Routing table for unicast routes
- A Routing table for multicast routes

The route table stores: <destination address, next hop address, destination sequence number, life time>.For each destination, a node maintains a list of precursor nodes, to route through them. Life-time updated every time the route is used. If route not used within its life time then it expires.

In AODV, source(S) first encounters the route to destination by broadcasting route request (RREQ) packet to its neighbour. This RREQ packet contains source node's IP address, source node's current sequence number, destination IP address, destination sequence number and broadcast ID number. Broadcast ID gets incremented each time a source node uses RREQ. Node A receives RREQ packet and makes entry for reverse route for S (dest=S, nexthop=S, hopcount=1).Since A has no routes to D, so it rebroadcasts RREQ packet to its neighbour nodes. Node C receives RREQ packet from A. It then makes a reverse route entry for S (dest=S, nexthop=A, hopcount=2) and it has a route to D so node C sends route reply (RREP) packet back on the reverse route to A and then to S. Then S sends message to D from the route discovered.

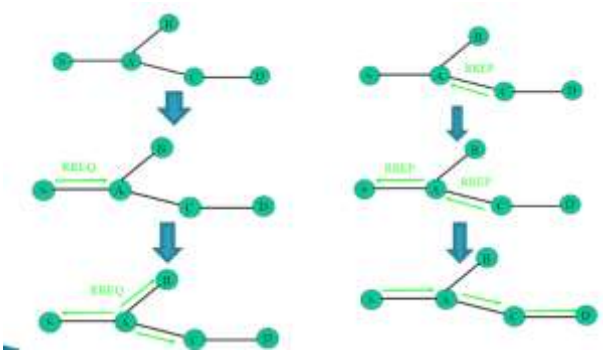

Fig.1 Message Transmission Using AODV Protocol

III. PROPOSED WORK

In this paper we have taken 10 nodes under a wireless sensor network. We have added faults of certain duration in nodes where number of nodes with fault increases with time. So we have taken 5 situations in which number of faulty nodes in the network are zero, two, four, seven and ten which are denoted by 0 faults , 2 faults ,4 faults, 7 faults, 10 faults. In 0 faults scenario we have not added any fault on any node. In 2 faults scenario faults are added to 4th node and 8th node for (400-550) sec and (200-350) sec respectively. In 4 fault scenario on 4 nodes fault is added i.e. 2nd node for (200-350) sec, 4th node for (50-150) sec, 6th node for (500-650) sec, 9th node for (800-950) sec. Similarly for 7 faults and 10 faults 7 nodes and 10 nodes are made faulty and there time duration is given in following table.

TABLE I
FAULT NODES

No. of nodes containing faults	Node number having fault	Duration
0	-	-
2	4th	(400-550)sec
	8th	(200-350)sec
4	2nd	(200-350)sec
	4th	(50-150)sec
	6th	(500-650)sec
	9th	(800-950)sec
7	1st	(0-250)sec
	3rd	(50-150)sec
	4th	(300-650)sec
	6th	(600-850)sec
	7th	(680-830)sec
	8th	(300-600)sec
	10th	(650-900)sec
10	1st	(0-500)sec
	2nd	(600-1000)sec
	3rd	(670-820)sec
	4th	(300-450)sec
	5th	(500-950)sec
	6th	(200-730)sec
	7th	(900-1500)sec
	8th	(200-350)sec
	9th	(850-1000)sec
	10th	(0-400)sec

TABLE II

SCENARIO PARAMETERS

Parameter	Value
Number of sensor nodes	10
Network Area	(1500*1500)m
Number of transmission packets	9
Number of fault nodes	3
Simulation time	1000sec
Node distribution	Random
Traffic generator	Zigbee
Mobility	No

In the scenario below10 nodes are shown with in a network and message is passed from 1st node to 10th node.

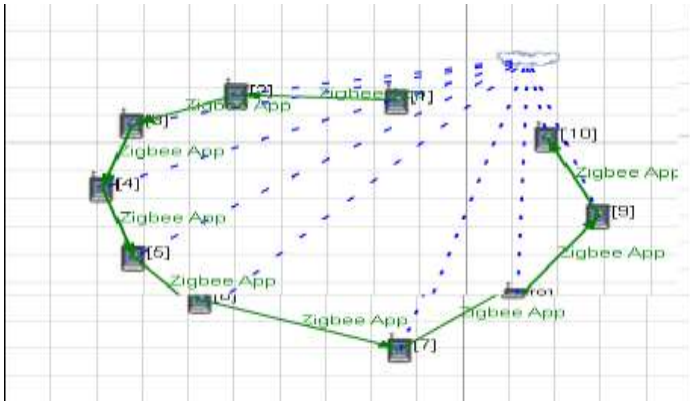

Fig.2 Scenario

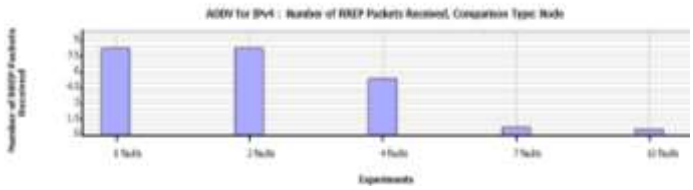

Fig.3 Number of RREP Packets Received

Number of hello messages received will also decrease as the number of faults in the network increases.

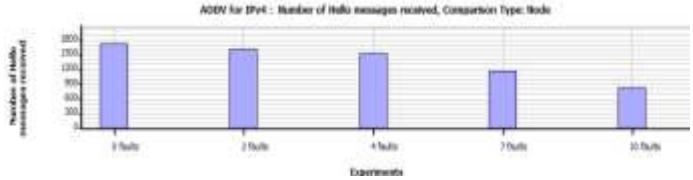

Fig4 Number of Hello messages received

Data packets are dropped when they are unable to reach to the sink node. Number of data packets dropped for no route increases with increase in number of faults in the network.

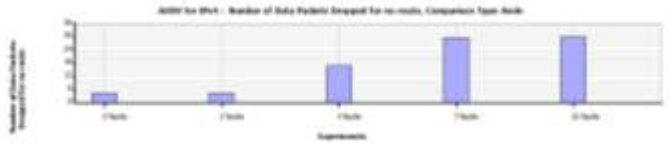

Fig5: Number of Data packets dropped for no route

Total number of hop counts for all routes decreases with increase in number of fault nodes in the network.

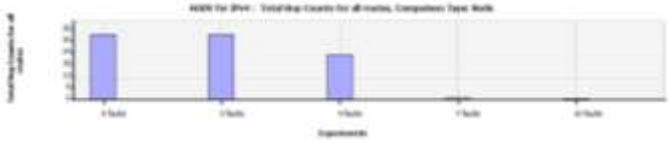

Fig.6 Total hop count for all route

As the number of faults increases in the network number of times link broke in the network also increased.

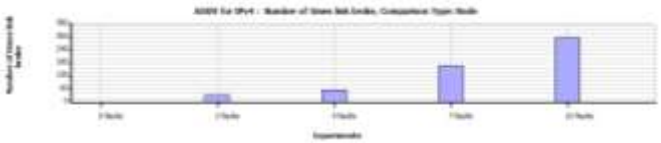

Fig.7 Number of times link broke

Signals received but with errors decreases with number of increase in fault nodes in the network.

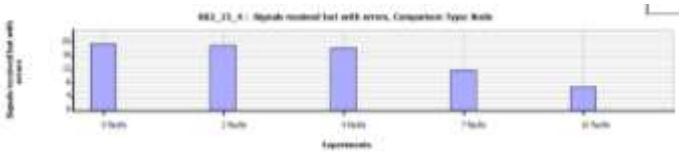

Fig.8 Signals Received But With Errors

Average end to end delay once increased when we had 4 faulty nodes in the network and then decreased when we had 7 faulty nodes and 10 faulty nodes in the network.

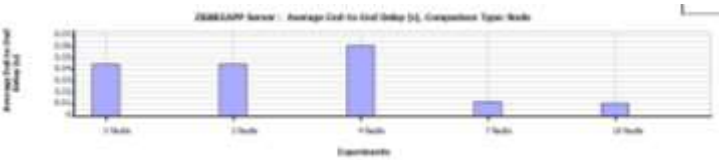

Fig.9 End To End Delay

Throughput that is number of bits sent per sec also don't have any criteria. According to our scenario throughput remains same for 2 faults scenario and then decreased for 4 faults scenario and again increased for 7 faults and 10 faults.

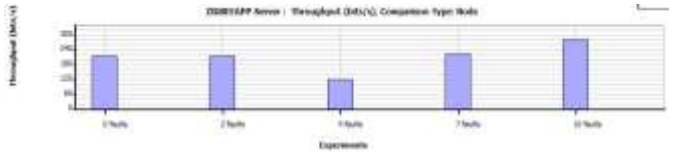

Fig.10 Throughput (bits/s)

The implementation developer must understand not only the routing protocol, but all the system components and their complex interactions.

IV. CONCLUSION

We have seen from above results that as no. of faults in the network increases, number of time link broke and no. of packets dropped for no route increases. Number of RREQ packets received, number of hello messages received, total hop count for no route and signals received but with errors decreases with increase in number of faults.

V. FUTURE WORK

In future we can try making a fault free network because faulty network decreases the life of network and increases efforts and time taken to accomplish the task.

REFERENCES

[1] S. Gobriel. "Energy-efficient design of ad-hoc and sensor networks", M.Sc, University of Pittsburgh, 2008

[2] Y. Chen and Nasser.“Enabling QoS multipath routing protocol for wireless sensor networks,” in IEEE International Conference, 2008, pp. 2421 – 2425.

[3] T. Zia and A. Zomaya. “Security issues in wireless sensor networks,” in Proceedings of the international Conference on Systems and Networks Communication, 2006.

[4] Y. Wang, G. Attebury and B. Ramamurthy.“A survey of security issues in wireless sensor networks,” IEEE communication surveys, Vol.8, No.2, 2006.

[5] A.al-yasiri and A.sunley. “Data aggregation in wireless sensor networks using the SOAP protocol,” Journal of Physics Conference Series 76, 2007.

[6] A.Khetrapal, “Routing techniques for Mobile Ad Hoc Networks Classification and Qualitative/ Quantitative Analysis,” Department of Computer Engineering, Delhi College of Engineering University.

[7] M. N. Elshakankiri, M. N. Moustafa and Y. H. Dakroury.“Energy Efficient Routing Protocol for Wireless Sensor Networks,” in International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Dec. 2008, pp. 393 – 398.

[8] F.L. Lewis, “wireless sensor network,” Technologies Protocols and Applications, New York, 2004.

[9] A. Habib. “Sensor network security issues at network layer,” in 2nd International Conference on Advances in Space Technologies Islamabad, Pakistan, Nov. 2008, pp. 58-63.

[10] A. A. Ahmed, H. Shi and Y. Shang. “A survey on network protocols for wireless sensor networks,” in Proceedings of Information Technology: Research and Education, Aug. 2003, pp. 301- 305.

[11] G. Acs and L. Buttyabv. “A taxonomy of routing protocols for wireless sensor networks,” BUTE Telecommunication department, Jan. 2007.

[12] M. Lyas and I. Magoub.Compact wireless and wired sensor system.CRC Press, 2004.