Special Issue of International Journal of Computer Applications (0975 – 8887)
on Wireless Communication and Mobile Networks, No.5. Jan.2012, ww.ijcaonline.org

Analysis of effects of Mobility and Active Route Timeout between Sensor Nodes in Wireless Sensor Networks

Meenakshi Tripathi
Dept of Comp Engg.,
MNIT,Jaipur

M. S. Gaur
Dept of Comp Engg.,
MNIT,Jaipu

Vijay Laxmi
Dept of Comp Engg.,
MNIT,Jaipur

Email: {Indian.meenakshi, gaurms, vlgaur@gmail.com}

ABSTRACT
Wireless sensor networks consists of thousands of tiny, low cost, low power and multifunctional sensor nodes where each sensor node has very small battery life. Routing in these networks has been active area of research. Due to dynamic nature of the wireless sensor networks, it is suggested to use reactive routing protocols. One of the popular reactive routing protocols is AODV which is being used with wireless sensor networks. In AODV route discovery overhead is minimized by caching the route for some time after a connection expires and how long each node would keep this information is set by a parameter, ACTIVE-ROUTE-TIMEOUT. We analyzed the performance of AODV by varying the value of ACTIVE_ROUTE_TIMEOUT from one second to several seconds with the mobility of sensor nodes. Extensive simulation has been done to better characterize the value of ACTIVE-ROUTE-TIMEOUT.

General Terms
Wireless sensor networks, algorithm, routing.

Keywords
Wireless Sensor network, routing algorithm, Active Route Timeout, Throughput, My Route Timeout, Qualnet.

1. INTRODUCTION
Wireless sensor networks consists of thousands of tiny, low cost, low power and multifunctional sensor nodes, each of which can sense various ambient conditions such as temperature, pressure, humidity, sound, lighting etc. and can communicate with each other through wireless medium. Sensor nodes are usually scattered in a region. Each sensor node has the capability to sense the data, compute some result and then communicate the result to the sink ([1],[2],[3]). Data are routed back to the end user by a multihop infrastructure less architecture through the sink. The sink may communicate to the task manager node via internet or satellite. The applications of sensor networks are quite numerous. Military applications, Environmental applications, natural habitat monitoring of birds [4], Biological applications: to monitor the glucose level, to detect the cancer, organ monitor, general health monitor etc.

One of the key challenges for wireless sensor network is security. Due to less computational and power capacity of sensor nodes it is difficult to implement any heavy security solution to these networks. So researchers are thinking to secure these kind of networks using some lightweight solutions.

The rest of the paper is organized as follows: Section 2 describes the routing issues of sensor networks, section 3 describes the taxonomy of routing protocols for sensor networks, section 4 gives the details of AODV routing protocol, section 6 describes the details of the simulation and the results and in the last the conclusion of the paper is presented.

2. ROUTING ISSUES IN SENSOR NETWORKS
Routing in sensor network is very challenging due to their specific characteristics. *First*, sensor networks are power constrained. Sensor nodes have small energy reserves. All communications even passive listening have a significant impact on those reserves. So to maximize the lifetime of the network, it is critical to maximize the usefulness of every bit transmitted or received. *Second*, these networks are expected to be highly dynamic in nature. Over time sensors may fail or new sensors may be added. Sensors are likely to experience change in their position, reachability, available energy, and even task details. These changes make static configuration unacceptable, the network must automatically adapt to changes in environment and requirements. *Third,* sensor networks must be self-configuring. Because of their deployment in large numbers or in places which are out of reach of a human being, the manual handling of the sensor nodes is not practical. *Fourth,* lack of global addressing scheme. Because of their dense nature it is very difficult to employ any global addressing scheme of wired networks. So traditional IP based protocols may not be applied to WSN's. An address-free architecture is proposed [5] for these networks, where nodes or data are described by attributes rather than addresses. *Fifth,* generated data traffic has significant redundancy in it since multiple sensors may generate same data within the vicinity of a phenomenon. Such redundancy needs to be exploited by the routing protocols to improve energy and bandwidth utilization. *Sixth,* the number of nodes deployed in the sensing area may be in the order of hundreds, thousands, or more and routing schemes must be scalable enough to respond to events. *Seventh*, Sensor networks are application-specific. In some application (e.g. some military applications), the data

should be delivered within a certain period of time from the moment it is sensed, while in other application (e.g. home security systems) the information should be sent only when an intruder is detected. Finally, Sensor networks can be deployed in hostile territory, where they can be subject to communication surveillance and node capture and compromise by adversaries. So routing algorithm must need to be designed in such a way that these security problems can be avoided.

3. TAXONMY OF ROUTING PROTOCOLS IN SENSOR NETWROKS

Proactive routing protocols maintains fresh list of destinations and their routes by exchanging the routing tables throughout the network. They react very slowly to any changes in the network. But in case of reactive routing protocols the routes are formed only when there is some data to transmit and route discovery is done by flooding the network with the route request packets. Hybrid protocols are combination of reactive and proactive protocols. We worked upon the reactive routing protocol: AODV (Ad Hoc On-Demand Distance Vector) routing protocol.

In broadways routing protocols[6] for sensor network can be divided into two categories flat routing and hierarchical routing depending on the network structure. In flat routing protocol each node plays the same role in the network, no hierarchy is there. Sensor networks are power constrained so multihop routing is used to send the data from various nodes to the sink. While in hierarchical routing protocols some sensor nodes are assigned special functionalities than other nodes in the network. This is achieved by cluster formation. A cluster consists of a set of geographically proximal sensor nodes; one of the nodes serves as a cluster head. The cluster heads can be organized into further hierarchical levels.

Depending upon whether the routing protocol is exploiting the location information of sensor nodes in calculating the routes or not the protocols can be location aware or location less protocols. Flooding-based protocols rely primarily on flooding for route discovery. Many protocols couple query routing with data routing, i.e. source nodes transmit their observed data readings directly in response to queries from sink nodes. Such protocols can be classified as query-driven protocols. On the other hand, data-driven protocols assume that there is a separate query propagation phase by which some sensor nodes realize that their data should be sent to a sink. This phase is generally also responsible for setting up routes. Source nodes transmit their readings along these routes either periodically or whenever they observe some interesting events during the subsequent data transfer phase Multipath routing protocols attempt to construct several completely or partially disjoint paths from the source to the sink. This increases the resilience of the network to node failures. Some routing protocols try to achieve QoS requirement along with the routing function, these are known as QoS routing protocols**.**

4. AODV ROUTING PROTOCOL

AODV [7][8] is an "On Demand Routing Protocol "means routes are discovered between source and destination only when source want to transmit some data Due to this reactive nature of protocol it reacts quickly to link breakages and changes in network topology so it is widely used with sensor networks. It works in two stages : Route Discovery and Route Maintenance stage. I Route Discovery stage, It discovers the route by sending RREQ (Route Request) and RREP (Route Reply) messages. While to maintain the established route it uses HELLO messages and RERR (Route Error) messages.

When source want to send some data to the destination it broadcasts RREQ to find the route to the destination. A route can be determined when the RREQ reaches either the destination itself, or an intermediate node with a 'fresh enough' route to the destination. A 'fresh enough' route is an unexpired route entry for the destination whose associated sequence number is at least as great as that contained in the RREQ. The route is made available by unicasting a RREP back to the source of the RREQ. Each node receiving the request caches a route back to the originator of the request, so that the RREP can be unicast from the destination along a path to that originator, or likewise from any intermediate node that is able to satisfy the request.
RREQ contains broadcast id, source IP address, source sequence number, destination IP address, destination sequence number and hop count. Source IP address and broadcast-id uniquely identifies any RREQ.After receiving the RREP the source node start transmitting the data to the destination.

To know about active neighbors each neighboring nodes periodically exchange HELLO messages. When a link break occurs while the route is active, all active neighbors are informed and link failures are propagated by means of route error (RERR) messages to the source node, which also update destination sequence numbers. After receiving the RERR message, the source node invalidates the route and can reinitiate route discovery, if desired.

When the source node broadcast a route request (RREQ) over the network, and the destination unicasts a route reply (RREP) to the source, the intermediate nodes store a route state between the source and the destination. Each node keeps this state for a length of time given by the parameter ACTIVE-ROUTE-TIMEOUT.

Every time the route is used, the timer is reset to back to the ACTIVE-ROUTE-TIMEOUT. If before this timer expires, the due to link layer failure or mobility of nodes the route breaks, AODV invalidate it. When link failure happens, AODV initiates a route error (RERR) process, which notifies the source with the invalid route.
The ACTIVE-ROUTE-TIMEOUT is a static parameter that defines how long a route is kept in the routing table after the last transmission of a packet on this route. This default value of this parameter is 2 seconds.

While selecting the value of ACTIVE-ROUTE-TIMEOUT, we need to keep a balance because a small value can start a new route discovery even if a valid route is still available, and a large value can create a risk of sending the packets on an invalid route. In the first case, the cost is the initiation of a new route discovery that could be avoided, and in the second case it is the loss of one or more packets and the initiation of a RERR process instead of a new route discovery without losing any packet.

In this document, we highlight the above trade-off and

Analyze the effect of ACTIVE-ROUTE-TIMEOUT on various performance parameter of the protocol. The results are obtained by performing extensive simulations on QUALNET 5.0.

5. SIMULATION ENVIRONMENT

We simulated the wireless sensor network using Qualnet 5.0 simulator which is a standard tool set used for wired, wireless, MANETs, and sensor networks. In our topology sensors are deployed randomly in a specified region, which are getting sensory information from the environment. These sensors are transmitting their data to mobile vehicles as and when they come into their range. this communication is according to 802.15.4 standard. These mobile vehicles then relay the data to ground station, which is a long distance communication based on 802.11. All the sensors are using 802.15.4 standard for PHY and MAC layer. Table 1 gives the details of parameters used for the simulation.

Simulation Parameter	Value
Dimension of Space	500 x 500
Number of Sensor nodes	100
Number of mobile Nodes	5
Ground station	1
Channel frequency	2.4 GHz
Simulation Time	30 min
Traffic Type	UDP
Number of CBR Connections	10
Data Packet Size	70 bytes
Path Loss Model	Two Ray Model
Mobility Model	Random Way Point
Speed	0 m/s,10m/s,20m/s

Table 1 : Simulation Parameters

51 Performance Metrics

While simulation our focus was to show the relationship between the mobility and the value of ACTIVE-ROUTE-TIMEOUT on the various performance parameters of the protocol. The following parameters are considered for simulation:

1. ***Packet Delivery Ratio (PDR)***: Packet delivery ratio is the fraction of packets sent by source that are received by the destination and is calculated by dividing the number of packets received by the destination through the number of packets originated by the application layer of the source. It's higher value indicates good performance of the protocol.
2. ***Average End to End Delay:*** End-to-end delay indicates how long it a packet takes to travel from the CBR source to the application layer of the destination. [9]. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, propagation and transfer times.
3. *Throughput*: The throughput is defined as the total amount of data a receiver receives from the sender divided by the time it takes for the receiver to get the last packet. The throughput is measured in bits per second (bit/s or bps) [10]
4. ***Average Jitter:*** Jitter [11] is the variation in the time between packets arriving, caused by network congestion, timing drift, or route changes. It should be less for a routing protocol to perform better.
5. *Total Bytes Received:* Number of received bytes by all nodes in the network for finding the target information [11].

6 Simulation results

Our simulation compares the effect of Active Route Timeout and node mobility on various performance metrics Figure 1 shows the PDR for an average node velocity of 0, 10 and 20 m/s. As the mobility of nodes which are collecting the data increases the PDR decreases. If the value of Active Route Timeout is less than 1, then in all the cases PDR is minimum since routes are cached for minimum amount of time.

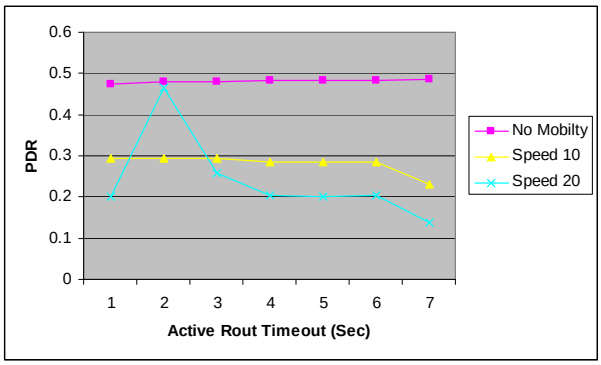

Figure 1: Active Route Timeout Vs PDR

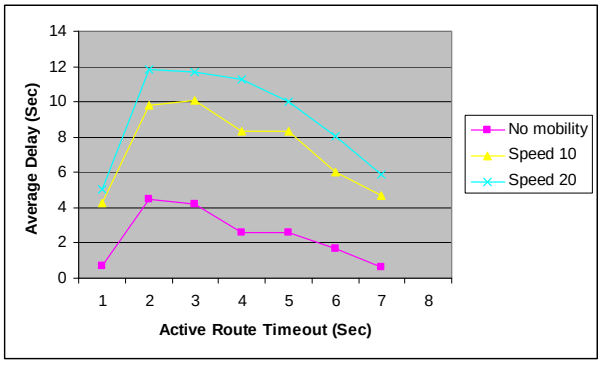

Figure 2: Active Route Timeout Vs Average Delay

As shown in Figure 2, Average delay of reaching the packet from source to the destination also increases with the mobility of nodes and achieves the highest value when Active Route Timeout is 1in all the cases. As we increase the value of Active Route Timeout, cached route expires late so the Average delay for a packet decreases.

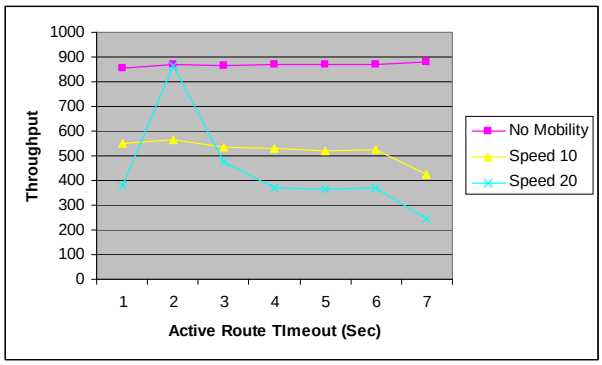

Figure 3: Active Route Timeout Vs Throughput

According to Figure 3 with speed 20 m/s and Active Route Timeout 1 we achieve highest throughput since more sensor nodes are coming into the range of mobile nodes. After it due to link errors there is a decrease in throughput.

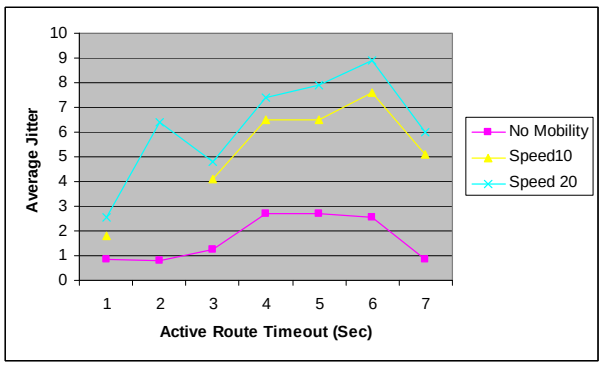

Figure 4: Active Route Timeout Vs Average Jitter

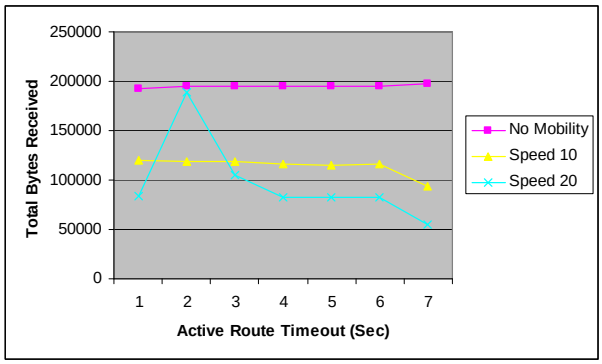

Figure 5: Active Route Timeout Vs Total Bytes Received

The value of total bytes received decreases when the Active Route Timeout is greater than 6.beceause of the more broken links.

7 CONSLUTION

We observe and argue that if the active route timeout is exactly 1 second then it provide maximum throughput. When we change the value of Active Route Timeout from 1 second to 5 seconds it gives almost same throughput since the routes are being cached for this much amount of time but after it decreases the throughput because of more link breaks. The other parameters also changes on variable values of Active Route Timeout. In Future we can simulate the effect of other static parameters of AODV like HELLO_INTERVAL, NET_DIAMETER, and RREQ_RETRIES. As well as we can see the effect of Active Route Timeout on different traffic patterns like bursty traffic.

8. REFERENCES

[1] Sayed Ahmed. Trlabs report : Current research on sensor networks. Technical report, TRLabs (Telecommunication Research Labs), Winnipeg, Manitoba, Canada, May 2004.

[2] I.F. Akyildiz, W.Su, Y.Sankarasubramaniam, and E.Cayirci. Routing techniques in wireless sensor networks: A survey. Computer Networks: The International Journal of Computer and Telecommunications Networking}, 38(4):393--422, March 2002.

[3] Deepak Ganesan, Alberto Cerpa, Wei Ye, Yan Yu, Jerry Zhao, and Deborah Estrin. Networking issues in wireless sensor networks. Journal of Parallel and Distributed Computing}, 64(7):799--814, 2004.

[4] Mainwaring, J. Polastre, R. Szewczyk, and J. Anderson D. Culler.Wireless sensor networks for habitat monitoring. In ACM International Workshop on Wireless Sensor Networks and Applications, Atlenta, Georgia, USA}, September 2002.

[5] J. Elson and D. *Estrin*. "An *Address-Free Architecture* for Dynamic *Sensor Networks*". Technical Report 00-724, Computer Science Department, USC, January 2000.

[6] Jamal, Ahmed E kamal "Routing techniques in wireless sensor networks: a survey ", *IEEE Wireless Communications*, Vol. 11, No. 6. (20 December 2004), pp. 6-28

[7] draft-ietf-manet-aodv-09.txt

[8] Charles E. Perkins and Elizabeth M. Royer. "Ad hoc On-Demand Distance Vector Routing." Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100, New Orleans, LA, February 1999.

[9] David Oliver Jorg, "Performance Comparison of MANET Routing Protocols In Different Network Sizes", Computer Science Project, Institute of Computer Science and Applied Mathematics, Computer Networks and Distributed Systems (RVS), University of Berne, Switzerland, 2003

[10] U. T. Nguyen and X. Xiong, "Rate-adaptive Multicast in Mobile Ad-hoc Networks," IEEE International Conference on Ad hocand Mobile Computing, Networking and Communications 2005 (WiMob 2005), Monreal, Canada, August 2005

[11] Scalable Network Technologies, —QualNet simulator 5.0 Version, tutorial on http://www.cs.binghamton.edu QualNet/qua lnet-tut1.pdf.