International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 1, Issue 3, November 2014

ERT-Enrichment Routing Technology for Wireless Sensor Network Using TEAODV

M.Uma Devi[1], D.Yamini[2], M.Joselin Rubia[3]
PG Student, M.E-Applied Electronics, SCAD College of Engineering and Technology, Tirunelveli, India[1]
Assistant Professor, Electronics and Communication Engineering, SCAD College of Engineering and Technology, Tirunelveli, India[2]
PG Student, M.E-Applied Electronics, SCAD College of Engineering and Technology, Tirunelveli, India[3]

Abstract: Wireless Sensor Networks (WSN) are applied in various field but the packet transmission is a major problem. In existing protocols, packet transmission occurs, but has less efficiency and there is a need for packet transmission also results in high energy consumption. Hence Trust based Energy aware Ad hoc on demand Distance Vector (TEAODV) is designed to overcome these failures. In this method is based on trust values. The nodes and routes with high trust are selected. Here the packet is transmitted efficiently from source to destination with high delivery ratio and low energy consumption. The performance of the proposed protocol has been evaluated and analyzed in terms of delivery ratio, packet drop, average energy, throughput for different number of nodes by considering trusted path along with path having minimum energy level nodes and shortest route. The performance of the protocol is implemented in wireless sensor network is shown with the help of NS2 Simulator.

Index Terms: Trusted path, reliable and energy efficient packet delivery, minimum energy level nodes, shortest path.

1. Introduction

Wireless Sensor Networks have drawn a lot of attraction due to its broad applications in military and civilian operations. It is a highly distributed network, having small size, light weight wireless nodes that are randomly deployed in large numbers to monitor the environments or systems [1] [2]. Their broadcast nature is used to gather data from the abutting environment and transmit it to the featured nodes called as sinks. Sensor networks consists of several types of sensors such as seismic, thermal visual, infrared, optical etc., They monitor a variety of physical parameters such as temperature, humidity, pressure etc., Sensors are also capable of capturing fast changing events in the world such as video, audio streams. Besides the challenging characteristics of WSN nodes, the constraint is that WSN nodes have limited power and memory capacity. The varying wireless channel conditions and sensor node failure may cause network topology and connectivity changes over time, to forward packet reliability at each hop, it may need multiple retransmissions. This results in undesirable delay and additional energy consumption. It is possible to delivery packets efficiently with available limited power by using trusted path and trusted node transmission. In AODV, the header packet containing only the next hop address is transmitted form source to destination, this process improves the performance of network with larger nodes. Routing path is selected in Ad-hoc On-demand Distance Vector (AODV) by using routing methods like route discovery and route maintenance [3]. In this paper, ad-hoc on demand routing with trust based mechanism which uses node trust and route trust is proposed. This scheme helps to protect nodes from sinkhole attacks in sensor networks. The paper is organized as follows: Section 2 explains about the ad-hoc on demand distance vector routing. Section 3 describes about trust scheme and selection of route. Section 4 deals with the main design. Results are discussed in Section 5 and a conclusion is given in section 6.

II. Ad-Hoc On-Demand Distance Vector Routing

In wireless sensor networks, routing protocol are classified as reactive and proactive routing. In reactive routing, the routes are created only when source wants to send data to destination, whereas pro active routing is table driven [4]. AODV belongs to reactive routing protocol and it uses traditional routing tables which has one entry per destination and destination sequence numbers. These entries are used to determine whether routing information is up-to-date and to prevent routing loops, which increases the efficiency of routing. It consist of two routing phases, they are route discovery and route maintenance.

A. Control Messages

It is used for the discovery and breakage of route and they are HELLO messages, Route Request Message (RREQ), Route Reply Message (RREP) and Route Error Message (RERR). HELLO messages are broadcasted in order to know neighborhood nodes, which communicate directly [5]. Route Request packet is flooded when there is a packet to forward but it has no routes to forward them to destination. RREQ is identified by the pair of source address and request ID, each time when the source node sends a new RREQ and the request ID is incremented. After receiving of request message, each node checks the request ID and source address pair. The new RREQ is discarded if there is already RREQ packet with same pair of parameters. On having a valid route to the destination or if the node is destination, a RREP message is sent to the source by the node as shown in Fig. 1. When a node receives an RREP, it checks if it is the selected next-hop of the RREP. If that is the case, the node realizes that it is on the guide path to the source thus it marks itself as a guide node. Then the node records its upstream guide node ID for this RREP and forwards it. In this way, the RREP is propagated by each guide node until it reaches the source via the reverse route of the corresponding RREQ. Finally, this process finds a guide path from the source to the destination. The neighborhood nodes are always monitored. When a route that is active, is lost then the neighborhood nodes are notified by route error message (RERR) on both sides of link.

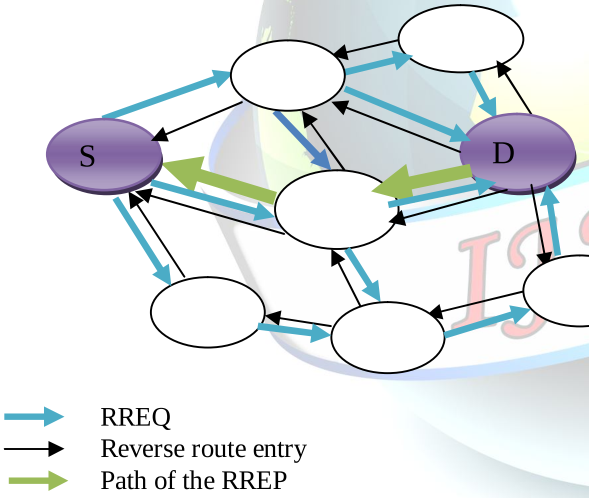


Fig. 1. Route discovery

There are two modes in route maintenance (a) Periodic broadcast of HELLO packets to their neighbors, and (b) uses acknowledgement mechanisms at link or network layers. Route error message contains the list of not reachable destinations.

III. Trust Scheme And Selection Of Route

The enhanced version of trust based ad hoc on demand distance vector routing protocol available for ad-hoc networks and WSN is implemented in the energy aware reactive routing protocol for different number of nodes and malicious nodes [6]. There are two trust values associated with the Trust based Energy aware Ad hoc on demand Distance Vector (TEAODV) protocol. They are route trust and node trust.

A. *Route Trust*

Route trust is the measure of the reliability with which a packet efficiently reaches the destination and it is computed by every node for each node but it is initially unknown. Source sends RREQ which helps in establishing the route to destination. RREQ have G flag, it is set to establish the reverse route from D to S. Each node keeps the track of the number of forwarded packets through the route. D periodically sends ACK packets to S at a particular interval which is readable by every node. Each intermediate node on the reverse route from destination to source checks the ACK packets to compute its route trust. Therefore route trust is calculated as a ratio of the number of packets received at D to the number of packets forwarded by the node.

B. *Node Trust*

Every node maintains node trust on each of its neighbor, based on which a route is selected for transmission. The number of route request is directly based on the node trust. The network setup is similar to AODV. Initially a node cannot judge its neighbors trust. So, 50% node trust is assigned to every node till the end of initial time. Node trust is calculated based on the difference between Advertised Trust Value (ATV) and Observed Trust Value (OTV) calculated for current data transfer. When a node X forwards or generates RREP, the node advertises its trust on the route with consideration to its immediate upstream node Y. The advertised trust value is denoted as ATV of node X. Then comparison between ATV and OTV takes place. Transmission takes place only if OTV is within the range of ATV or else the node X is penalized. If there is only one node between source and destination, then only that particular node is responsible for the packets to reach the destination. Its trust value is based on its behavior and its link to the destination.

C. Route Selection Method

Source node S receives number of route reply packets in response to its route request to destination node D. Source node calculates Route Selection Value(RSV) for all its available routes to destination. Then Source node selects the route having highest RSV. If two routes have same RSV value then following rules is used

I. The routes having high trust value is preferred for transmission.

II. If two route have same trust value then route with highest immediate neighbor node is selected

III. If the immediate neighbor node is also same then shortest route is selected

IV. If there is two shortest paths, then random selection based on RSV is made.

IV. MAIN DESIGN

In main design, the route request, route reply and route error message is explained with help of flow chart.

A. Route Request And Route Error Flow

Route request is forwarded from source to destination with the help of intermediate nodes. Route error message is send when there is a break in the flow of messages or if the transmission line breaks. If a source node has a packet to send then it initiates by flooding RREQ which is identified by the pair of source address and request ID. If it is route request, then the nodes checks whether it is the destination. A new RREQ is discarded if there is already a RREQ packet with same pair of parameters.

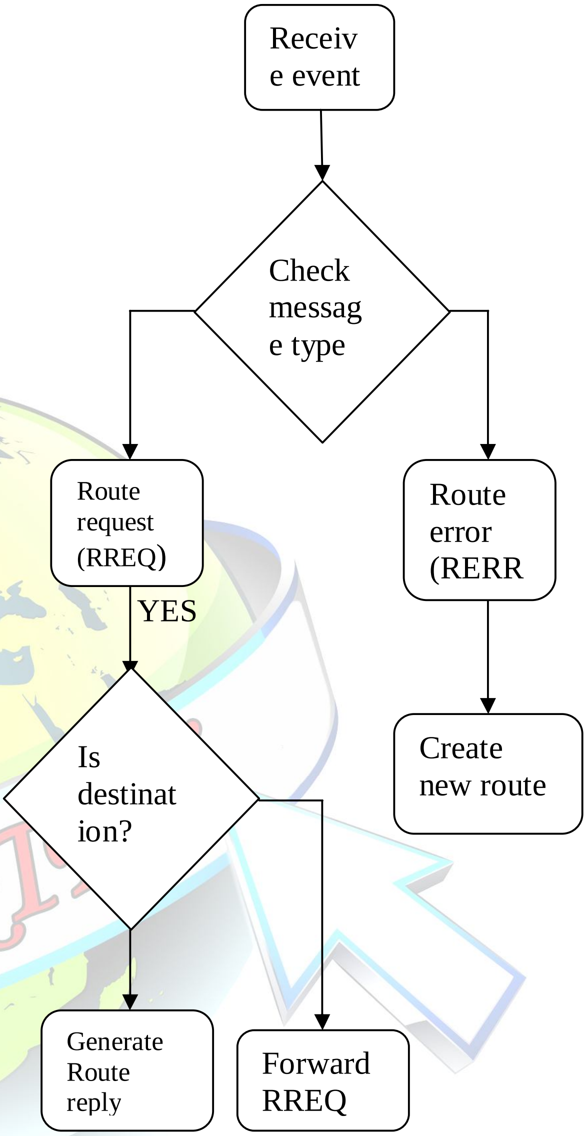


Fig. 2. Flow chart for RREQ and RERR

When a node receives an event, it first checks for the message type whether it is a route request or route reply or route error as shown in Fig. 2. If it is found as RERR message, then new route is created. RERR occurs due to breakage of link or loss of packets. When a route that is active is lost, the neighborhood nodes are notified by route error message on both sides of link.

B. Route Reply

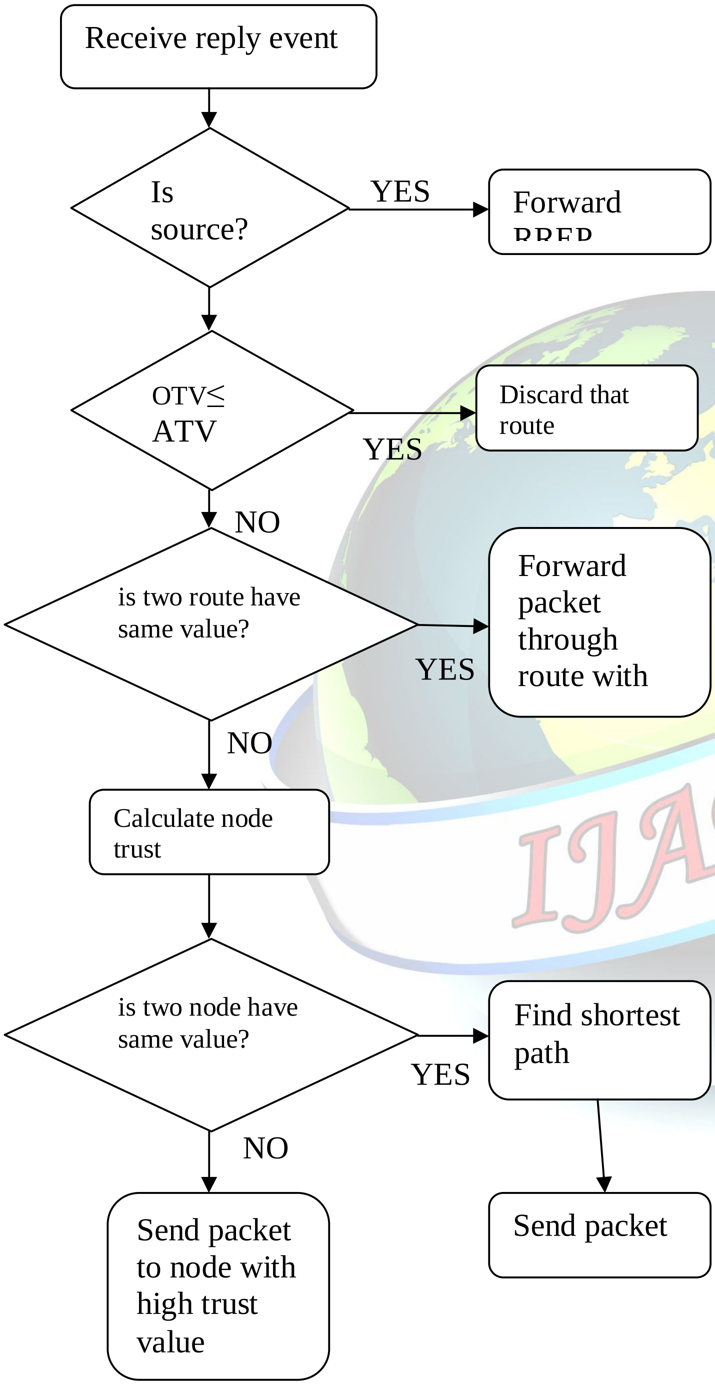


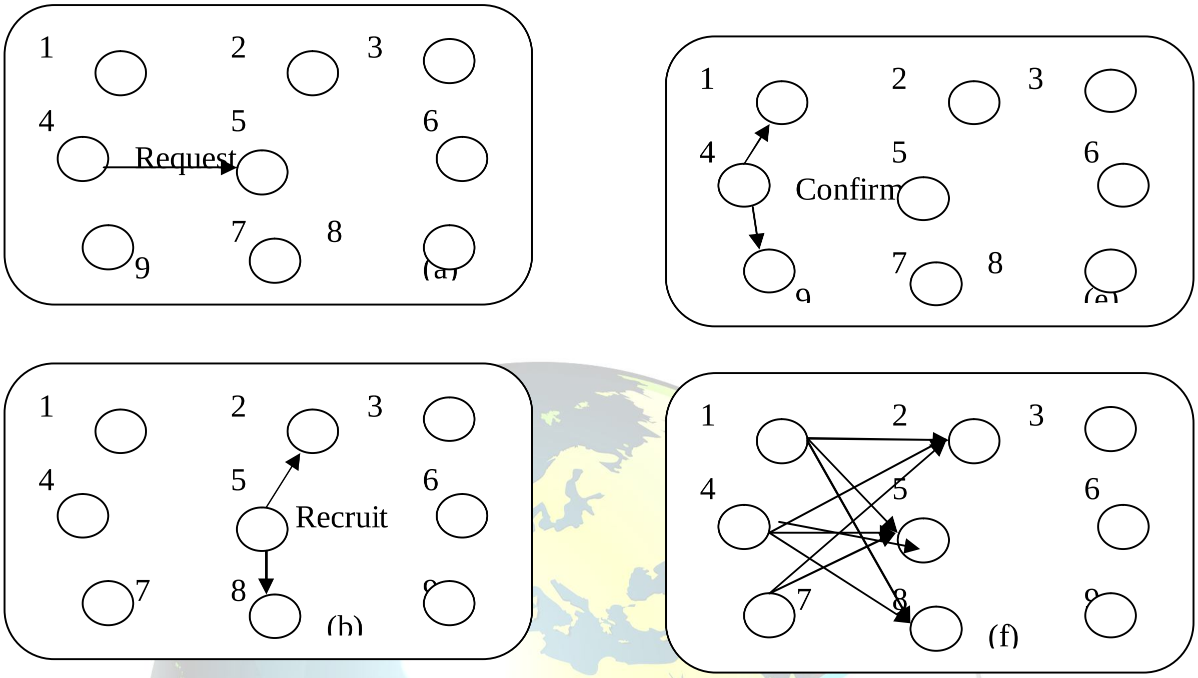
Fig. 3.Flow chart for RREP

If there is a valid route from destination to source, RREP message is send to the source with the help of intermediate nodes. When a node receives an RREP, it checks if it is the selected next-hop of the RREP. If that is the case, the node realizes that it is on the guide path to the source, thus it marks itself as a guide node. Then, the node records its upstream guide node ID for this RREP and forwards it. In this way, the RREP is propagated by each guide node until it reaches the source via the reverse route of the corresponding RREQ, which gives guide path. The destination generates route reply and passes to the source. Every node when gets the RREP message, node checks whether it is the source node as shown in fig 3.

If it is the source node then check whether the advertised trust vale and the observed trust value matches. If that particular node is not the source node then the node forward RREP message. If ATV has greater value than OTV then the particular route is discarded or else transfers through the route having highest value. When two routes have same route trust, then the node trust is calculated. Then node transfer packet to high node trust value. If node trust is also same then the packet is transferred to the shortest path.

C. RECRUIT And Transmit Phase

This phase takes place after route reply is completed. This phase helps to recruit and transmit the packet through the shortest path. The nodes which recruit additional adjacent intermediate node are called cluster head. This is a dynamic process and done for every packet. If there is a packet to be sent, the cluster head initiates the recruiting by the next node on the one-node-thick path. The next node is called a receiving cluster. Once when this receiving cluster is identified, the packet transmission takes place between transmitting and receiving cluster nodes. The operations are request to recruit, sending of recruit packet, passage of grant packet followed by clear and confirm packet and the last step of process is to send the data packets.



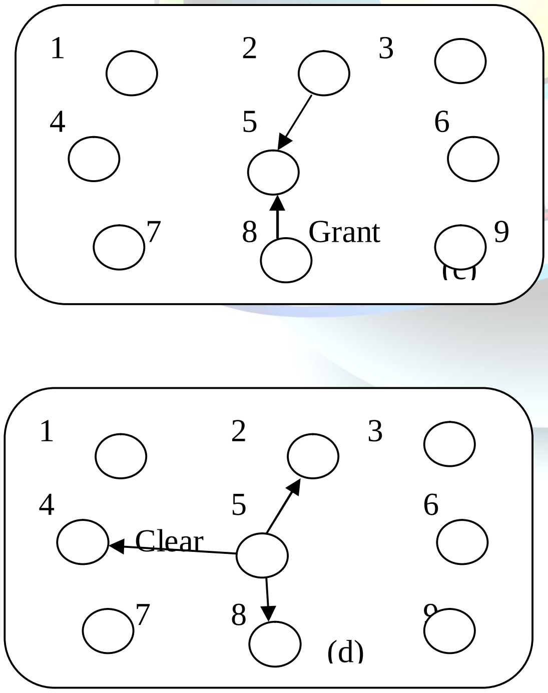


Fig. 4. Example for recruiting phase operation (a) Request-to-recruit (RR) packet (b) Recruit (REC) packet (c) Grant (GR) packet (d) Clear (CL) packet (e) Confirm (CF) packet (f) Transmission of the data packet.

In the example shown in Fig. 4 the node is the sending cluster head and node 6 is the receiving cluster head. When the node 4 has the packet to send then it forwards request to recruit (RR) packet to node 5 as shown in Fig. 4(a). When it receives RR packet it starts to form the receiving nodes. Then as shown in Fig. 4(b), the node 5 forwards recruit (REC) packet to node 2 and 8. Once the node 2 and 8 receives the REC, it calculates the cost from the sending cluster head to the particular node and the cost from that node to receiving cluster head. Node 2 calculates the cost of (4, 2) and (2, 6) similarly for node 8, the cost is (4, 8) and (8, 6). Then node 2 and 8 sends grant (GR) packet with the calculated costs as shown in Fig. 4(c). The number of nodes which receives REC packet is denoted as m and if the number of grant is less than m-1 then the entire REC packet received nodes are selected to form the receiving clusters. After receiving the cost, node 5 sends clear (CL) packet to the nodes 4, 2, 8 with the IDs of cooperating nodes 2 and 8 as shown in Fig. 4(d). From the Fig. 4(e) node 4 sends confirm packets to enable the packet transmission. After receiving the confirm packets, nodes 1, 4, 7 sends the data packet as shown in Fig. 4(f).

V. Simulation Results

For an efficient packet transmission, there must not be a need for packet retransmission and the packet transmission rate must be high with less power consumption. The simulation results for TEAODV throughput, average energy, and packet delivery ratio along with packet drop are obtained with the help of NS2 simulator. The node first transmits the RREQ to all the neighborhood nodes until the destination node is reached. Then RREP packets is forwarded to source then the recruit and transmit phase takes places. Then the transmission takes place with high efficiency.

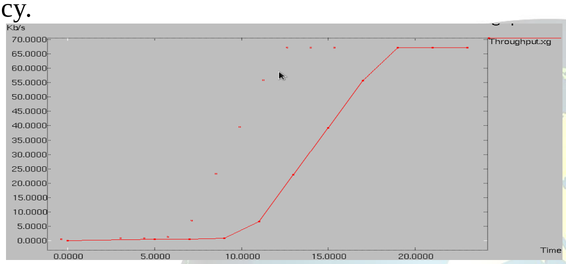


Fig. 5(a). Throughput

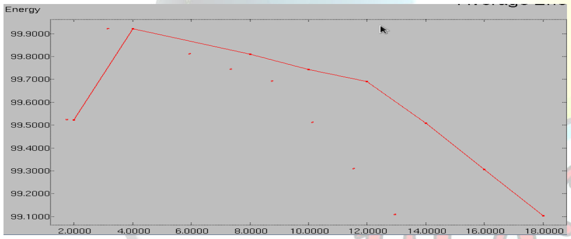


Fig. 5(b).Average energy

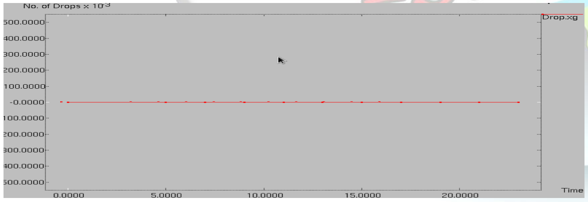


Fig. 5(c). Packet drop

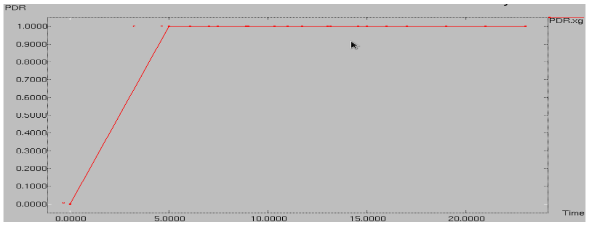


Fig. 5(d). Packet delivery ratio

From fig. 5(a), Packet transmission rate increases with respect to time which is known. From fig. 5(b), it is clear that average energy consumption is decreases with time. Packet drop does not take place which is known from fig. 5(c) and there is no need for packet retransmission. Since packet drop does not occur packet delivery ratio as shown in fig. 5(d).

VI.Conclusion

In this work, a protocol method which provides higher efficiency than other protocols is presented. Thus, it helps in energy-efficient packet delivery in WSN. In this paper a trust based routing scheme that helps in finding the robust virtual transmission path with low overhead is introduced. Data packets can be transferred to destination without the help of local information. Therefore, TEAODV provides high routing performance than other routing protocol and performance with respect to average energy, throughput, packet drop and packet delivery ratio is also shown.

Acknowledgment

We thank the lord Almighty for his grace to us. We also thank our parents, friends for their support and encouragement.

References

[1]. K. Low, W. Win, and M. Er, "Wireless sensor networks for industrial environments," in *Proc. Int. Conf. Intell. Agents, Web Technol. Internet Commerce*, Nov. 2005, vol. 2, pp. 271–276.

[2]. A.Willig, "Recent and emerging topics in wireless industrial communications: A selection," *IEEE Trans. Ind. Inf.*, vol. 4, no. 2, pp. 102 124, May 2008.

[3]. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. IEEE WMCSA*, 1999, pp. 90–100. D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Computing*, pp. 153–181, 1996.

[4]. Royer and C.-K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," *IEEE Pers. Commun.*, vol. 6, no. 2, pp. 46–55, 1999.

[5]. J. Heo, J. Hong, and Y. Cho, "Earq: Energy aware routing for real-time and reliable communication in wireless industrial sensor networks," *IEEE Trans. Ind. Inf.*, vol. 5, no. 1, pp. 3–11, Feb. 2009.

[6]. Y. Gu and T. He, "Dynamic switching-based data forwarding for lowduty- cycle wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 10, no. 12, pp. 1741–1754, Dec. 2011.