LIGHTWEIGHT ROBUST ROUTING IN MOBILE WIRELESS SENSOR NETWORKS

Xiaoxia Huang, Hongqiang Zhai and Yuguang Fang
Department of Electrical & Computer Engineering
University of Florida

ABSTRACT

In mobile wireless networks, path breakage happens frequently due to the movement of mobile nodes, node failure, channel fading and shadowing. It is challenging to combat path breakage at the cost of minimum control overhead, while adapting to topological changes rapidly. Due to the Wireless Broadcast Advantage, all nodes inside the transmission range of the transmitting node may receive the packet. Inherently, those nodes serve as cooperative caching and backup nodes if the intended receiver fails to receive the packet. In distributed robust routing, presented here, nodes work cooperatively to enhance the robustness of routing against path failure. Our simulation results show that robust routing improves robustness in mobile wireless sensor networks while achieving energy efficiency.

INTRODUCTION

Wireless sensor network is envisioned to be essential to many applications. Most of current research assumes wireless sensor networks to be stationary, however, in some scenarios, wireless sensor networks must be mobile. For instance, in wild life applications, sensors are cast in the field as well as equipped on animals to be monitored. The self-organized wireless sensor network is mobile as animals are moving around. In telemedicine applications, sensors attached to patients also constitute a mobile wireless sensor network. As expected, mobile wireless sensor network is more difficult to deal with than its stationary counterpart. In mobile wireless networks, path breakage happens frequently due to channel fading, shadowing, interference, node mobility as well as node failure. When a path breaks, rerouting or resorting to a backup route is necessary and should be carried out as soon as possible. Otherwise, packet loss and large delay would occur. Different types of routing protocols have been proposed for mobile wireless ad hoc networks. But they are not suitable for highly dynamic topologies especially for energy and computation capability constrained sensor nodes. Therefore, prompt path recovery, energy efficiency and robustness are highly preferred characteristics for routing protocols in mobile wireless sensor networks.

After initially establishing a path between source and destination nodes, robust routing is able to provide reliable packet delivery against path breakage. Packets can be delivered towards the destination immediately in spite of link break. As a distributed approach, robust routing is relieved from the substantial control overhead for route maintenance and update. Light overhead is incurred during the procedure of robust routing. Without requirement on location information, it is relatively insusceptible to node mobility. The best relay node is self-elected on a per-packet basis. Through cooperation among neighboring nodes, the energy efficiency is also improved since more reliable and stable links are preferred in relay. Thus, our robust routing protocol is resistant to link error. Choosing reliable links potentially reduces retransmissions, thus saving energy and shortening delay. Through cross design with MAC layer, our robust routing is more energy and delay efficient than routing protocols purely relying on network layer design. Simulation result demonstrates that our robust routing protocol improves performance visibly in presence of node mobility and link error.

The rest of the paper is organized as follows. Section II discusses previous work on related topics. Section III describes the Wireless Broadcast Advantage of wireless medium. Section IV illustrates the robust routing scheme. Section V demonstrates and discusses the simulation results. Section VI concludes the paper.

RELATED WORK

There is some initial work on cooperative communication and routing. But most of them focus on physical layer, such as mitigating multipath fading, increase SNR at the receiver, efficient encoding and decoding and etc. ExOR [2] is proposed to increase the throughput in multi-hop wireless networks to take advantage of multiple forwarders. Maintaining a prioritized forwarder list at source and intermediate nodes, forwarders relay successfully received packets in order of priority. Our scheme does not need the knowledge of relaying nodes, so it better adapts to

This work was supported in part by the U.S. Office of Naval Research under Young Investigator Award N000140210464.

mobile and error-prone wireless sensor networks. In [5], a modified version of AODV over specialized IEEE 802.11 MAC protocol is proposed to explore path diversity which strengthens the path reliability. Multiple receiving nodes are assigned with certain priority at each hop. Among the nodes having received the packet, the one with the highest priority is the relay node. Combining a MAC protocol capable of channel-state based next hop selection [6] with AOMDV [12], the proposed method could deal with packet loss due to channel error. Zhu and Cao [4] utilize multi-hop relay at MAC layer to achieve higher throughput given multi-rate physical links. Assuming nodes are rational, Srinivasan and et. al [3] apply game theory to the problem of cooperation of energy constrained nodes for packet relay. The proposed algorithm converges to the optimal operating point which trades throughput with lifetime. The authors [1] work on the cross design of physical communication and routing. A set of cooperating nodes are selected to transmit to a set of receiving nodes at each stage with the objective to minimize energy consumption. Inherently, cooperative routing is more efficient when it utilizes physical or MAC layer information. In our paper, MAC layer is incorporated in routing protocol design.

In mobile wireless ad hoc network, topology varies frequently. To deal with path breakage, usually a large amount of overhead is generated to maintain path information or reroute. So many routing protocols are not readily applicable in mobile wireless sensor networks. DSDV [7], AODV [8], DSR [9], ZRP [10] are the most well known routing protocols for mobile ad hoc networks. Many follow-on works are proposed to further improve the performance. In [11], a combination of ant-routing and AODV is proposed to reduce route discovery latency and end-to-end delay. Many routing protocols use alternative paths established in neighborhood when the primary path fails. Modifications of AODV are proposed to better address frequent link failures due to mobility in MANETs. AODV-BR [14] builds up fish-bone like structure through overhearing RREP transferred along the primary path. Backup paths with two hop difference from the primary path are set up in the route discovery phase [15]. AOMDV [12] establishes multiple path at one time, so alternative paths can be used in case of path failure. As an extension of ZRP [10], two-zone routing protocol [13] decouples the protocol's ability to adapt to traffic characteristics from the ability to adapt to mobility. Our work is different from the previous work because it does not invoke network-wide rerouting in order to provide robustness and energy efficiency. Cooperation nodes are not predetermined and unknown to the sender, but autonomously selected based on link quality in the routing process.

WIRELESS BROADCAST ADVANTAGE

Due to the broadcast nature of wireless medium, neighboring nodes of a transmitting node may receive the packet with only one transmission. This phenomenon is called Wireless Broadcast Advantage (WBA) [16], which is illustrated in Fig. 1. Intuitively, those neighboring nodes can cooperate to perform robust and energy efficient routing because they keep a copy of the same packet with no additional cost. Inherently, it is also cooperative caching in the neighborhood. As nodes with a copy behave as cache, the next-hop node could retrieve the packet from any of them. Suppose source node s attempts to deliver a packet to destination node d over path $s-1-2-d$. After s has transmitted to node 1, nodes 3 and 4 receive the packet too. Since multiple nodes obtain a copy of the packet, they create transmission side diversity. Cooperation among those nodes may result in energy-efficiency and robustness if we carefully harness the diversity.

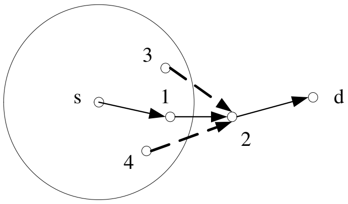

Figure 1. Illustration of WBA

ROBUST ROUTING

In robust routing, multiple nodes with the same packet try to deliver it to another node cooperatively. Assume all nodes have the same transmission range. Suppose a path is established between source and destination nodes at the beginning. In our scheme, we use the shortest path between the source and destination nodes. The established path is referred to as the intended path. Similarly, nodes on the intended path are called intended nodes. A guard node is at least a neighboring node of two intended nodes. In other words, a guard node can reach at least two intended nodes. Likewise, a link between a guard node and intended node is called a guard link. The intended path, along with the guard nodes, collectively constitute the strong path, which is used for robust routing. A path is selected on the per packet basis in the strong path. Using multiple guard links, the robustness of an intended link is enhanced at each hop. Revisiting the example in Fig. 1, we briefly introduce the basic idea of robust routing. If link $(s, 1)$ fails due to such as deep fading or node 1 departure, then node 1 cannot receive the packet correctly. However, through guard nodes 3 and 4, its downstream node 2 may still receive the packet successfully. Without several retransmissions over the unreliable or expired link $(s, 1)$ before dropping the packet, a substitute link $(3, 2)$ or $(4, 2)$ could forward the packet immediately. As long as at least one link is able to deliver the packet, the packet can be received and further forwarded towards the destination. Actually, robust routing is actually forwarding in a zone. Nodes in the area covered by guard nodes collaboratively forward the packet to the next area progressively towards the destination. Different from traditional narrow path consisting of one node at each hop, the strong path contains multiple nodes at each hop, as shown in Fig. 2.

To sum up, when an intended node fails to receive a packet from its intended upstream node, guard nodes who successfully receive the packet will collaborate to redeliver the packet instead of retransmissions. If the packet can be directly transmitted to the intended downstream node by a cooperation node, this would shorten delay and save energy because of the saved transmissions. Fig. 1 best illustrates the idea. Through node 3 or 4, the number of transmissions needed from node s to node 2 reduces to 2 if links transfer the packet successfully. Otherwise, the total number of transmissions needed from node s to 2 would be at least 4, if node s only retransmits to node 1 once and switches to another path, say $s - 4 - 2$, thereafter. The probability that all guard links and the intended link fail simultaneously is much smaller than the probability of a failed intended link. Therefore, guard links are able to improve reliability at the cost of spending more energy in overhearing at guard nodes. On the other hand, potential energy savings by avoiding retransmissions over a hostile or disappeared link offsets the energy consumption for overhearing. It is possible that cooperation among guard nodes lowers the energy consumption while achieving robustness.

The basic idea is straightfoward, but we need to deal with cross layer design in order to coordinate involved guard nodes. Rather than purely relying on the network layer to implement cooperation, MAC and network layer cooperation can achieve better channel utilization and energy efficiency. Our robust routing is different from multicast or anycast, because cooperation nodes have the knowledge about the succeeding nodes. So the trace of a packet is restricted in the strong path, instead of propagating in the whole network randomly.

A. Strong path

After an intended path is established between a source-destination pair, every intended node broadcasts partial path information to help construct the strong path. The broadcast information includes source node, destination node, node ID of current node, its upstream and downstream nodes. The source and destination nodes are used to identify an intended path. It is easy for a node to discover whether it is a neighbor of two intended nodes through overhearing ongoing transmissions. If a node hears transmissions, including control and data packets, from two different nodes belonging to the same intended path, it is eligible to participate in routing. Based on the broadcast information, the intended node within the transmission range of the guard node, which is relatively closer to the destination node is chosen to be its next-hop node. The closeness can be determined by the partial path information in the broadcast information. It then records its next-hop intended nodes and the source and destination nodes. This record is used to packet forwarding. If a node belongs to several strong paths, it maintains a record for each path. All guard nodes and intended nodes form a strip connecting the source and destination nodes. How nodes in the strip work together is illustrated in the next subsection. An example of building up a strong path is shown in Fig. 2. The shaded area shows the strong path formed between s and d. Guard nodes only appear in the strong path.

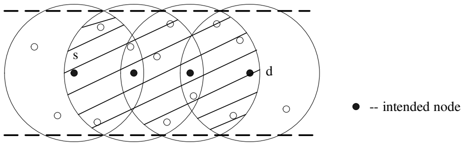

Figure 2. A strong path forms between s and d

B. Cooperation among guard nodes

Based on the relative location to the intended nodes, guard nodes can be classified into two categories, equivalent nodes and remedy nodes. The relative location determines the role and priority of a guard node in cooperation. The most preferred guard node can substitute an intended node if it is the neighbor of two-hop away intended nodes. This means that the guard node could bridge the upstream and downstream nodes of the corresponding intended node. When the substitutable intended node fails to relay the packet, the packet detours and goes through the guard node, then back to the intended path. Since those kind of nodes act as backup nodes of the intended nodes, this first tier is referred to as the equivalent nodes. Denote N_e the set of equivalent nodes.

We modify IEEE 802.11 to support our robust routing. RTS/CTS handshake works in the same way as in IEEE 802.11. After finishing data transmission, the sender waits for an ACK. If the intended receiver has successfully received the packet, it replies with an ACK after Short Inter-Frame Spacing (SIFS). Otherwise, the channel is silent during this interval. Hearing no ACK, a guard node learns that the intended link fails and replies an ACK to the sender for relaying if it has obtained a copy of the packet. This is the difference of our MAC from IEEE 802.11. Instead of only the intended receiver replying an ACK to the sender after a successful reception, the node eligible to help relay can reply with an ACK. The first replying node will be the sole relay node. Since the carrier sensing range is normally larger than the transmission range, the ACK can be heard or sensed by all other guard nodes. They know that some node will relay, so they keep silent to avoid collision. As long as a packet is received by at least one guard node, no retransmission is needed when the intended receiver fails to obtain the packet. The coordinated relay saves delay and energy when the intended link is in bad condition or failed.

It is possible that several nodes are equivalent nodes. To break the tie and reduce the potential collisions and energy waste caused by multiple redeliveries, equivalent nodes respond to the sender after differentiated backoff time, say T_{boe}. The backoff process is shown in Fig. 3. Obviously, the node with the shortest backoff time will be the first one replying with an ACK. Once other nodes that are counting down the backoff time hear or sense the ACK, they stop competing for relay. Thereafter, election for the relay node ends. The winner node then contends for the channel and initiates the relay. The backoff delay is shown in (1).

$$T_{boe,m} = SIFS + T_e V_m P_m, \text{ for node m} \in N_e \tag{1}$$

where,

$$P_m = \frac{D_m}{1 - E_m}$$

T_e is the backoff window for equivalent nodes. To better adapt to mobile environment, V_m is considered in relay. V_m is the relative mobility to the intended downstream node, ranging from [0.01, 1]. It is the normalized average relative moving speed during a time period. If zero is an allowed value, multiple resting nodes will take the same backoff time SIFS, which causes collision. So zero is not a valid value in the computation. A highly mobile guard node results in an unstable link. When the node is relaying, the link will break if it moves out of the transmission range of the receiver. So V_m is used as a prediction of the stability. A node with zero or low relative mobility is preferred as it is less likely to cause link breakage during a transmission. P_m is a mixed metric of normalized link delay D_m and error probability E_m of the link between node m and the downstream node of the failed intended node. E_m indicates link fading and shadowing. Link delay is the average delay experienced when forwarding a packet over the link. It also indicates the traffic load around the area. When the traffic is heavy, severe contentions happen. Consequently, a packet is expected to experience a long link delay. With these two factors, a link with less contention and higher reliability tends to be the relay node. Apparently, the backoff time for the first tier node is no greater than $SIFS + T_e$.

If no ACK is heard or sensed before T_e ends, it implies that no equivalent node can relay for current node. Now, the second tier nodes are allowed to compete for relay. The second tier, referred to as remedy nodes, contains the common neighbors of the current intended node and its downstream node, or neighbors of both the current intended node and an equivalent node. So when an intended node fails to receive a packet correctly, the packet may bypass the intended node and go through a remedy node. It travels through the remedy node, via the intended node or a guard node of the next-hop, returning to the downstream node on the intended path. Remedy nodes should keep silent until $SIFS + T_e$ expires. If no ACK is heard or sensed during this period, say $SIFS + T_e$, they assume that no equivalent node is available or eligible to relay. The second competition stage begins if no equivalent node transmits in the first stage. So guard nodes relay with differentiated priority. In the first stage, only first tier nodes can be active. Second tier nodes compete with an additional backoff delay T_e in the second stage. Denote N_r the set of remedy nodes and T_{bor} the backoff time for remedy nodes. Similar to equivalent nodes, they defer ACKs with backoff time

$$T_{bor,m} = SIFS + T_e + T_r V_m P_m, \text{ for node m} \in N_r \tag{2}$$

T_r is the backoff window for remedy nodes. Any remedy node hearing or sensing an ACK from another remedy node, assumes that a successful cooperation is completed. Then it just discards the received packet. The maximum backoff time for remedy nodes is $SIFS + T_e + T_r$. The time interval between the end of DATA transmission and ACK is bounded by this value. Therefore, the maximum time for a packet transmission after seizing the channel can be derived according to Fig. 3.

If an intended node continuously fails in reception for several packets, say 5, it is assumed to be away from the intended path or dead. It no longer qualifies for routing. The guard node recently accomplishing redelivery substitutes the failed node, and becomes the new intended node by broadcasting the same information as in the strong path formation phase. Then a new set of equivalent nodes and remedy nodes are constructed correspondingly. Former guard nodes outside of the range of the new intended node no longer hear transmissions from the former intended node because that node is opted out. Accordingly, they discard outdated information and quit routing after timeout.

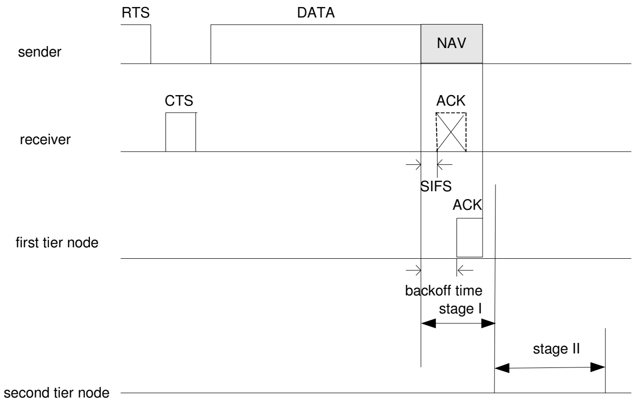

Figure 3. A first tier node is a relay node.

The backoff time for each guard node is unpredictable, but the maximum backoff time or competition period is controllable. If the relay node hears an RTS from another node before sending out the ACK, the DATA/ACK handshake may be interrupted. To avoid this situation, we modify the NAV(Network Allocation Vector) to a larger value. All nodes set the NAV as the sum of the NAV in IEEE 802.11, $NAV_{802.11}$, and the maximum backoff time T_{max} for cooperation, as

$$NAV = NAV_{802.11} + T_e + T_r = NAV_{802.11} + T_{max}$$

Since an ACK is sent out before NAV goes to zero if a relay node exists, NAV guarantees that current handshake process is not interrupted by nearby transmissions. The shortcoming of using the new NAV value is that even an ACK is sent back to the sender before NAV goes to zero, nodes still keep idle for the rest of NAV. But T_{max}, which is on the order of several hundred microsecond, is much smaller than the time for one retransmission(usually on the order of millisecond for 1K data packets), so our protocol still has a shorter delay than conventional retransmission schemes. The value of T_{max} depends on the network density. If the density is high, more nodes are potentially eligible for cooperation routing. Therefore, T_{max} should be large enough to reduce the probability of ACK collisions among relaying nodes. Nodes are widely differentiated with a large value of T_{max}, but the relay latency is relatively high. Using a small value, the relay delay decreases, but results in a high chance of ACK collisions at the backoff stage. Even there is a relay latency in our protocol, it may still save end-to-end delay because a retransmission usually costs more time to contend for channel and retransmit the large data packet.

SIMULATION

In this section, we compare the simulation result of our scheme with DSDV and AOMDV in NS-2. AOMDV establishes several alternative paths during path establishment as in AODV. We use three paths for each source-destination pair in AOMDV. If all three paths fail simultaneously, rerouting is performed. We use two-way ground model as the physical propagation model. 15 nodes are randomly deployed in a $600m \times 600m$ field. Two flows are randomly generated. As indicated by the trace file, the source-destination distance varies between 2 to 6 hops in simulations when nodes move around. The sources generate packets at a rate of 20packets/s with size of 1000 bytes. Every node moves according to the random-way point mobility model. The minimum speed of nodes is 1m/s. The maximum speed of each node changes from 5m/s to 20m/s in simulations to investigate the performance with respect to node mobility. A simulation lasts for 600-second. We compare packet delivery ratio, end-to-end packet delay and energy consumption per bit. The energy consumption per bit is the average energy consumed to send a bit from the source to the destination.

Fig. 4 shows the packet delivery ratio with respect to different degree of mobility. Our robust routing scheme outperforms DSDV and AOMDV up to 167% and 23%, respectively. The improvement is attributed to its responsiveness to topology changes. Although AOMDV establishes multiple backup paths to enhance the reliability against path breakage, it is possible that all paths fail simultaneously. As all nodes are mobile, it is very likely that some links on several discovered paths break ub a short time. Even the network is under saturated, packet loss is high because of the frequent path breakages caused by node mobility. DSDV experiences the greatest packet loss among the three because the established path may be outdated or no longer exist after a short period.

Robust routing performs better than AOMDV, but a little inferior to DSDV in terms of end-to-end delay, as shown in Fig. 5. In DSDV, packets are immediately forwarded upon receiving based on the routing information stored at each intermediate node. However, a packet has to wait until a path is available in AOMDV, so it tends to experience a longer delay. Our robust routing protocol actually selects an currently available path in the strong path through cooperation. Because there is a node election process, packets experience a longer delay than DSDV, but much shorter than AOMDV.

Observe in Fig. 6, the energy consumption per bit of our robust routing protocol increases as the node mobility

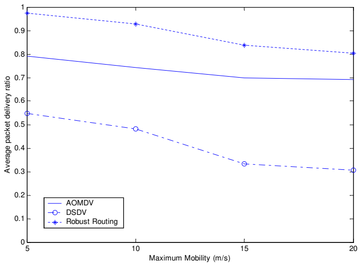

Figure 4. Packet delivery ratio vs node mobility

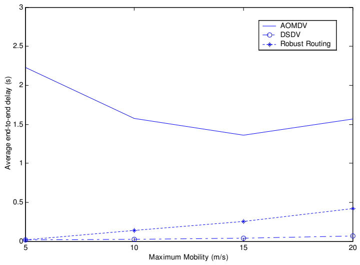

Figure 5. End-to-end delay vs node mobility

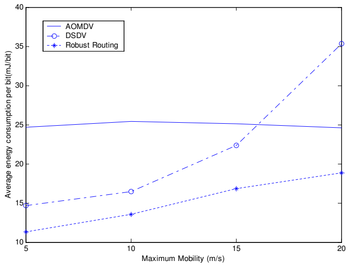

Figure 6. Energy consumption vs node mobility

increases. AOMDV is almost not affected by mobility in terms of energy consumption because overhead for path discovery does not change much with the node mobility. As expected, the energy consumption of DSDV increases with node mobility because frequent topology changes incur more overhead. The energy consumption of robust routing is lower than AOMDV at relatively low mobility, but slowly grows close to AOMDV as maximum node mobility increases. The reason is that a large amount of packets have to go through the cooperation process with high node mobility. The update messages are sent out more frequently by newly self-nominated node on the intended path to refresh path information. This also accounts for the rise in energy consumption.

CONCLUSION

This paper presents a cross-layer robust routing protocol based on node cooperation among nearby nodes for mobile wireless sensor networks. Based on the path quality, the intended path changes adaptively to the changing topology. The strong path changes with the intended path as well. Utilizing path diversity in the strong path, the robust routing protocol is capable of selecting the best path in a wide zone for each packet, which is different from traditional routing protocols. It is a distributed routing protocol and operates with moderate overhead. To support the novel routing protocol, we proposed a modified version of IEEE 802.11 MAC protocol. Nodes self-coordinate to elect the best forwarding node according to the link quality based backoff delay.

Potential future work includes integrating the robust routing with some path refreshing mechanism, which is used to discover a new intended path when performance of current intended path degrades to a certain level.

REFERENCES

[1] A. Khandani, J. Abounadi, E. Modiano and L. Zhang, "Cooperative Routing in Wireless Networks," Allerton Conference on Communications, Control and Computing, Oct. 2003.

[2] S. Biswas and R. Morris, "ExOR: Opportunistic Multi-Hop Routing for Wireless Networks," *SIGCOMM2005*, pp. 133-144, Philadelphia, PA, Aug. 2005.

[3] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini and R. R. Rao, "Cooperaton in Wireless Ad Hoc Networks," *INFOCOM2003*, vol. 2, pp. 808-817, San Francisco, CA, Mar. 2003.

[4] H. Zhu and G. Cao, "rDCF: A Relay-enabled Medium Access Control Protocol for Wireless Ad Hoc Networks," *INFCOM2005*, vol. 1, pp. 12-22, Miami, FL, Mar. 2005.

[5] J. Wang, H. Zhai, W. Liu and Y. Fang, "Reliable and Efficient Packet Forwarding by Utilizing Path Diversity in Wireless Ad Hoc Networks," *Proc. IEEE MILCOM*, vol. 1, pp. 258-264, Oct. 2004.

[6] S. Jain and S. R. Das, "Exploiting Path Diversity in the Link Layer in Wireless Ad Hoc Networks," *Proc. of the 6th IEEE WoWMoM Symposium*, pp. 22-30, Jun. 2005.

[7] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," *Proc. of SIGCOMM 94*, pp. 234-244, Aug. 1994.

[8] C. Perkins, E. Belding-Royer and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF RFC 3561, Jul. 2003.

[9] D. B Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," *Mobile Computing*, vol. 353, pp. 153-181, 1996.

[10] Z. J. Haas, "A New Routing Protocol for the Reconfigurable Wireless Networks," *Proc. of the IEEE Int'l Conf. on Universal Personal Comm.*, pp. 562-566, Oct. 1997.

[11] S. Marwaham, C. K. Tham and D. Srinivasan, "Mobile Agents Based Routing Protocol for Mobile Ad Hoc Networks," *Proc. IEEE GLOBECOM*, pp. 163-167, Nov. 2002.

[12] M. Marina and S. R. Das, "On Demand Multipath Distance Vector Routing in Ad Hoc Networks," *Proc. of the Int'l Conf. on Network Protocols(ICNP)*, pp. 14-23, Dec. 2001.

[13] L. Wang and S. Olariu, "A Two-Zone Hybrid Routing Protocol for Mobile Ad Hoc Networks," *IEEE Trans. on Parallel and Distributed Systems*, vol. 15, no. 12, pp. 1105-1116, Dec. 2004.

[14] S. J. Lee and M. Gerla, "AODV-BR: Backup Routing in Ad Hoc Networks,"*Proc. IEEE WNMC*, vol.3, pp. 1311-1316, Sept. 2000.

[15] H. Chen and C. Lee, "Two Hops Backup Routing Protocol in Mobile Ad Hoc Networks," *Proc. of the Int'l conf. on Parallel and Distributed Systems*, vol. 2, pp. 600-604, Jul. 2005.

[16] J. E. Wieselthier, G. D Nguyen and A. Ephremides, "Algorithms for Energy-efficient Multicasting in Ad Hoc Wireless Networks," *ACM/Springer Mobile Networks and Applications*, vol. 6, no. 3, pp. 251-263, June 2001.