International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 5, July - 2012

Performance Evaluation of Cooperative Robust Routing Protocol for Mobile Wireless Sensor Network

Mrs. Nilam Pradhan
Dept. Of E & TC
MIT college of Engg.
Pune, India

Charudatta Kulkarni
Dept. Of E & TC
MIT college of Engg.
Pune, India

Ramesh Mali
Dept. Of E & TC
MIT college of Engg.
Pune, India

Abstract

In mobile wireless sensor network (WSN) path breakage happens frequently due to mobility of nodes, node failure, interference and shadowing. Due to this packet loss and large delay would occur. Routing protocols are implemented for mobile wireless Ad Hoc network, are not suitable for highly dynamic topologies, especially for energy and computation capability constrained sensor nodes. This paper illustrates new distributed Robust Routing Protocol (RRP) that works cooperatively to enhance the robustness of the routing, which reduces total number of retransmissions and improve the energy efficiency. And compare performance parameters like packet delivery ratio and end-to-end delay of RRP with the existing routing protocol for different network scenarios. The work is carried out using network simulator NS2.34.

1. Introduction

Wireless sensor network (WSN) is an emerging technology used in many applications including habitat monitoring, industrial process monitoring, environment and healthcare applications, homeland security etc. WSN consists of low cost, small size and low powered sensor nodes which are deployed to places where traditional wired or wireless networks are not feasible. Most of current research assumes wireless sensor networks to be stationary however, in some scenarios wireless sensor networks must be mobile. For an instance, in wild life applications sensors are cast in the field as well as are equipped on animals to be monitored. The self-organized wireless sensor network is mobile as animals are moving. In telemedicine applications, sensors attached to patients also constitute a mobile wireless sensor network.

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. Many ad hoc routing protocols such as AODV, DSR, DSDR, TORA and OLSR, which have been developed particularly for the mobile wireless ad hoc networks (MANETs), performed satisfactorily on MANETs. 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.

This paper illustrates ‘Robust Routing Protocol’ which 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. It enhances the robustness of routing against path breakage. Light overhead is incurred during the procedure of robust routing. Through cooperation among neighboring nodes, the energy efficiency is also improved since more reliable and stable links are preferred in relay.

Previous work on related topics is discussed in section II. Section III presents the robust cooperative routing protocol design. Section IV illustrates experimentation for robust cooperative routing protocol in NS2.32. Result and discussion is clarified in Section V. Section VI concludes the paper.

2. Related Work

A number of routing protocols have been implemented like Destination- Sequenced Distance-Vector (DSDV) routing protocol, Ad Hoc On-Demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR) etc. for mobile wireless ad hoc network. In mobile wireless ad hoc network, topology varies frequently. To deal with path breakage, usually large amount of overhead is generated to maintain the path information or reroute. So many routing protocols are not readily applicable to mobile wireless sensor networks.

DSDV is based on the idea of the classical Bellman-Ford routing algorithm with some improvements. DSDV is a proactive, distance vector protocol. The primary characteristic of proactive approach is that each node has to maintain a route to every other node in the network all the times regardless of whether or not these routes are needed. Node maintains a routing table that lists all available destinations, the number of hops to reach the destination and the sequence number assigned by the destination node. The packets may be transmitted using either layer 2 (MAC) addresses or layer 3 (network) addresses. The main contribution of the algorithm was to solve the routing loop problem. DSDV requires a regular update of its routing tables, which uses up battery power and a small amount of bandwidth even when the network is idle.

AODV is a relative of the Bellmann-Ford distant vector algorithm, but is adapted to work in a mobile environment. It is reactive routing protocol. The network is silent until a connection is needed. AODV determines a route to a destination only when a node wants to send a packet to that destination. Routes are maintained as long as they are needed by the source. The network node that needs a connection broadcasts a request for connection. Other AODV nodes forward this message. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Disadvantage of this protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. Also, multiple RouteReply packets in response to a single RouteRequest packet can lead to heavy control overhead.

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. Dynamic Source Routing, DSR, is a reactive routing protocol that uses source routing to send packets. It uses source routing which means that the source must know the complete hop sequence to the destination. Each node maintains a route cache, where all routes it knows are stored. A negative consequence of this is the routing overhead every packet has to carry.

There is some initial work on cooperative communication and routing. Most of them focus on physical layer, such as mitigating multipath fading, increase SNR at the receiver, efficient encoding and decoding etc. ExOR 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. This scheme does not need the knowledge of relaying nodes, so it better adapts to mobile and error-prone wireless sensor networks.

AOMDV establishes multiple paths at one time, so alternative paths can be used in case of path failure. Combining a MAC protocol capable of channel-state based next hop selection with AOMDV; the proposed method could deal with packet loss due to channel error. Utilize multi-hop relay at MAC layer to achieve higher throughput given multi-rate physical links. The proposed algorithm converges to the optimal operating point which trades throughput with lifetime. 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 this paper, MAC layer is incorporated in routing protocol design.

3. Cooperative Robust Routing Protocol

RRP takes advantage of WBA. 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), which is illustrated in Fig. 1. Spontaneously, 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 - 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 use the diversity.

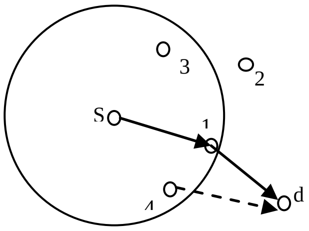


Figure 1.Illustration of WBA

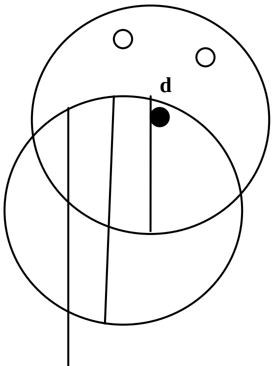
The basic idea of robust routing is if link (s, 1) fails due to such as deep fading or node 1 departure, then node 1 cannot receive the packet correctly. However, through guard nodes 4, its destination node d may still receive the packet successfully. Without several retransmissions over the unreliable or expired link (s, 1) before dropping the packet, a substitute link (4, d) 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.

When an intended node fails to receive a packet from its intended upstream node, guard nodes who successfully receive the packet will cooperate with each other 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. The probability that all guard links and the intended link fails 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.

In robust routing Protocol, 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 this scheme, the shortest path between the source and destination nodes is used. 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 constitutes 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. This work is different from the previous work because it does not invoke network-wide rerouting in order to provide robustness and energy efficiency.

3.1 Formation of Robust 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, and its upstream and downstream nodes. The source and destination nodes are used to identify an



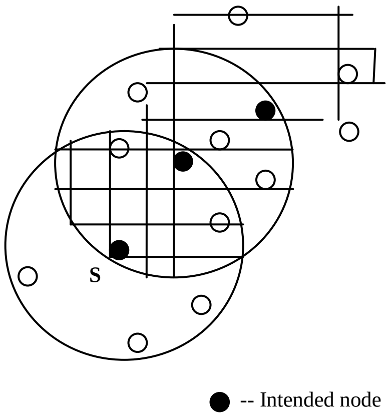


Figure 2. A strong path forms between s and d

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.

3.2 Cooperation among Guard Nodes

From the location of 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 that kind of nodes act as backup nodes of the intended nodes, this first level is referred to as the equivalent nodes. Denote Ne the set of equivalent nodes. MAC layer protocol IEEE 802.11 is modified to support 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 this 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 Tboe. 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).

$$\mathrm{Tboe,m} = \mathrm{SIFS} + \mathrm{TeVmPm} \qquad (1)$$
$$\text{for node } \mathrm{m} \in \mathrm{Ne}$$

Where,

$$\mathrm{Pm} = \frac{\mathrm{Dm}}{1-\mathrm{Em}}$$

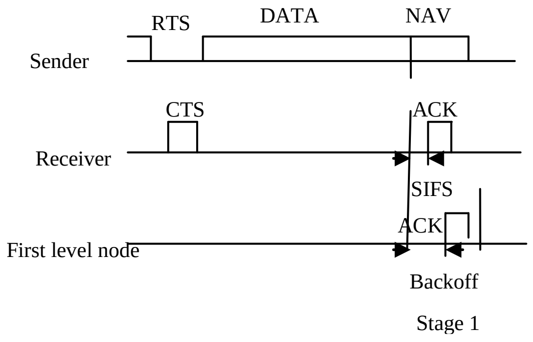


Figure 3. A first level node is a relay node.

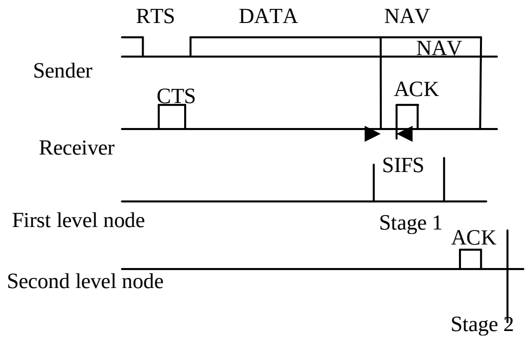


Figure 4. A second level node is a relay node.

Te is the backoff window for equivalent nodes. To better adapt to mobile environment, Vm is considered in relay. Vm 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. 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 Vm 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. Pm is a mixed metric of normalized link delay Dm and error probability Em of the link between node m and the downstream node of the failed intended node. Em 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 contention happens. 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 level node is no greater than SIFS + Te.

If no ACK is heard or sensed before Te ends, it implies that no equivalent node can relay for current node. Now, the second level nodes are allowed to compete for relay. The second level, 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 + Te expires. If no ACK is heard or sensed during this period, say SIFS + Te, 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 level nodes can be active.

Second level nodes compete with an additional backoff delay Te in the second stage. Denote Nr the set of remedy nodes and Tbor the backoff time for remedy nodes. Similar to equivalent nodes, they defer ACKs with backoff time

$$\begin{aligned}&\mathrm{Tbor,m}\\&=\mathrm{SIFS}+\mathrm{Te}\\&+\mathrm{TrVmPm},\quad \text{for node m Nr} \;\ldots\ldots(2)\end{aligned}$$

Tr 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 + Te + Tr. 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. 8. 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.

4. Performance Analysis

Simulation results of RRP along with DSDV and AOMDV in NS-2 shows that, AOMDV establishes multiple alternative paths during the path establishment stage. The packet delivery ratio and the throughput are measured.

As nodes in the robust path bear implicit geographic information about the intended path, they could react quickly to the link failure through cooperation. Although AOMDV establishes multiple backup paths to enhance the robustness against path breakage; it is possible that all paths fail simultaneously. As time elapses, paths become invalid. Since all nodes are moving, it is very likely that some links on several discovered paths break shortly. DSDV experiences the most serious packet loss among the three because it is a proactive algorithm. The established path may be outdated or no longer exist after a period. As in Fig. 5. The packet delivery ratio of robust routing decreases slightly as the mobility increases.

Robust routing performs better than AOMDV, but a little inferior to DSDV in terms of end-to-end delay. As a proactive routing protocol, routing information is stored at each intermediate node before packet arrival in DSDV. Therefore, packets are immediately forwarded upon reception. However, AOMDV is an on-demand routing protocol. A packet has to wait until paths are found, so it tends to experience longer delay. Robust routing protocol selects an available path in the established robust path through cooperation. Because there is a node election process during forwarding, packets experience longer delay than DSDV, but shorter than AOMDV.

Throughput or network is the average rate of successful message delivery over a communication channel. This data is pass through a certain network node.The throughput of robust routing protocol is better than AOMDV and DSDV. For densely deployed scenario, throughput is more in all three protocols.

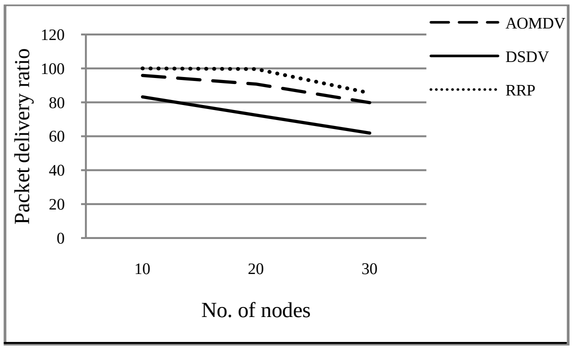


Figure 5. Packet delivery ratio.

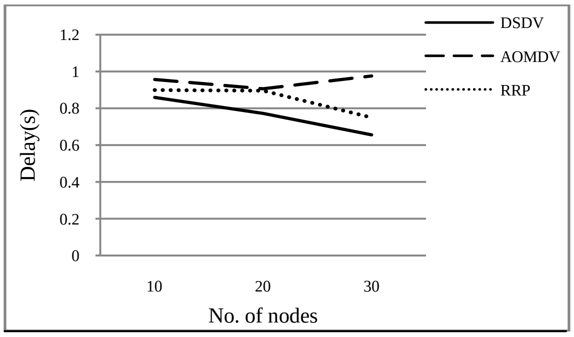


Figure 6. Delay.

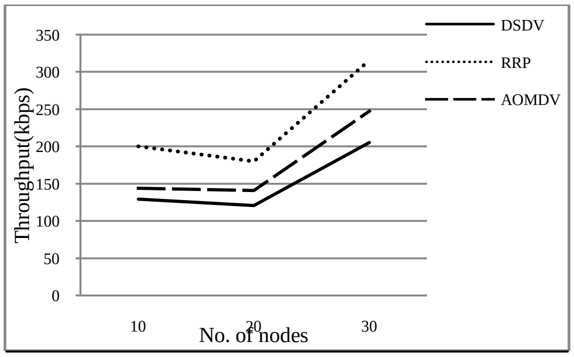


Figure 7. Throughput(kbps).

5. Conclusion

This paper presents a robust routing protocol based on node cooperation among nearby nodes for mobile wireless sensor networks. A reliable path is selected for packet delivery. Based on the path quality, the intended path is able to adapt to the varying topology. The robust routing protocol is capable of selecting the best path in a wide zone for each packet. Therefore, the robustness against path breakage is improved. The intended path changes adaptively to the changing topology. 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.

6. REFERENCES

[1] Xiaoxia Huang, Hongqiang Zhaiand Yuguang Fang, "Robust Cooperative Routing Protocol in Mobile Wireless Sensor Networks" *IEEE Trans. on Wireless Communications*, VOL. 7, NO. 12, pp.5278-5285 Dec. 2008.

[2] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *Proc. ACM SIGCOMM 1994*, pp. 234-244, Aug. 1994.

[3] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," IETF RFC 3561, July 2003.

[4] DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks *David B. Johnson David A. Maltz Josh Broch* Computer Science Department Carnegie Mellon University Pittsburgh, PA 15213-3891

[5] H. Kwon, T. H. Kim, S. Choi, and B. G. Lee, "A cross-layer strategy for energy-efficient reliable delivery in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 5, no. 12, pp. 3689-3699, Dec. 2006.

[5] J. Wang, H. Zhai, W. Liu, and Y. Fang, "Reliable and efficient packet forwarding by utilizing path diversity in wireless ad hoc networks," in *Proc. IEEE MILCOM*, vol. 1, pp. 258-264, Oct. 2004.

[7] A. Khandani, J. Abounadi, E. Modiano, and L. Zhang, "Cooperative routing in wireless networks," in *Proc. Allerton Conf. on Comm., Control and Computing*, Oct. 2003.

[8] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: efficient protocols and outage behavior," *IEEE Trans. Inform. Theory*, vol. 50, no. 12, pp. 3062-3080, Dec. 2004.

[9] S. Cui and A. J. Goldsmith, "Energy efficient routing based on cooperative MIMO techniques," in *Proc. IEEE Int'l Conf. on Acoustics, Speech, and Signal Processing 2005 (ICASSP 2005)*, vol. 5, pp. 805-808, Mar. 2005.

[10] Q. Qin and R. S. Blum, "Capacity of wireless ad hoc networks with cooperative diversity: a warning on the interaction of relaying and multihop routing," in *Proc. IEEE Int'l Conf. on Comm. 2005 (ICC 2005)*, vol. 2, pp. 1128-1131, May 2005.

[11] A. S. Ibrahim, A. K. Sadek, W. Su, and K. J. R. Liu, "Cooperative communications with relay-selection: when to cooperate and whom to cooperate with?" *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2814-2827, July 2008.

[12] S. Biswas and R. Morris, "ExOR: opportunistic multi-hop routing for wireless networks," in *Proc. ACM SIGCOMM 2005*, pp. 133-144, Philadelphia, PA, Aug. 2005.

[13] S. Jain and S. R. Das, "Exploiting path diversity in the link layer in wireless ad hoc networks," in *Proc. 6th IEEE WoWMoM Symposium*, pp. 22-30, June 2005.

[14] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, and R. R. Rao, "Cooperation in wireless ad hoc networks," in *Proc. IEEE INFOCOM 2003*, vol. 2, pp. 808-817, San Francisco, CA, Mar. 2003.

[15] X. Huang, H. Zhai, and Y. Fang, "Lightweight robust routing in mobile wireless sensor networks," in *Proc. IEEE MILCOM 2006*, Oct. 2006.

[16] L. Yin and G. Cao, "Supporting cooperative caching in ad hoc networks," *IEEE Trans. Mobile Computing*, vol. 5, no. 1, pp. 77-89, Jan. 2006.

[17] M. Marina and S. R. Das, "On demand multipath distance vector routing in ad hoc networks," in *Proc. Int'l Conf. on Network Protocols(ICNP)*, pp. 14-23, Dec. 2001.

[18] L. Wang and S. Olariu, "A two-zone hybrid routing protocol for mobile ad hoc networks," *IEEE Trans. Parallel and Distributed Systems*, vol. 15, no. 12, pp. 1105-1116, Dec. 2004.

[19] S. Bohacek, "Performance improvements provided by route discovery in multihop wireless networks," *IEEE Trans. Mobile Computing*, vol. 7, no. 3, pp. 372-384, Mar. 2008.