Robust Cooperative Routing Protocol in Mobile Wireless Sensor Networks

Xiaoxia Huang, *Member, IEEE*, Hongqiang Zhai, *Member, IEEE*, and Yuguang Fang, *Fellow, IEEE*

***Abstract*—In wireless sensor networks, path breakage occurs frequently due to node mobility, node failure, and channel impairments. It is challenging to combat path breakage with minimal control overhead, while adapting to rapid topological changes. Due to the Wireless Broadcast Advantage (WBA), all nodes inside the transmission range of a single transmitting node may receive the packet, hence naturally they can serve as cooperative caching and backup nodes if the intended receiver fails to receive the packet. In this paper, we present a distributed robust routing protocol in which nodes work cooperatively to enhance the robustness of routing against path breakage. We compare the energy efficiency of cooperative routing with non-cooperative routing and show that our robust routing protocol can significantly improve robustness while achieving considerable energy efficiency.**

***Index Terms*—Robustness, routing, wireless sensor networks, mobility.**

I. Introduction

WIRELESS sensor networks are envisioned to be essential to many applications and will impact our daily life significantly. In many application scenarios, wireless sensor networks must be mobile. As an example, in wildlife monitoring or environmental study, sensors are cast in the field as well as are equipped on free-ranging animals to be monitored. In mobile wireless networks, path breakage occurs more frequently due to channel fading, shadowing, interference, node mobility as well as power failure. When a path breaks, rerouting or alternative routing may be necessary and should be carried out promptly. Otherwise, packet loss and large delay would occur. Different types of routing protocols have been proposed for mobile wireless ad hoc networks. However, 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.

Manuscript received September 6, 2006; accepted October 2, 2008. The associate editor coordinating the review of this paper and approving it for publication was D. Zeghlache.

This work was partially supported by the US National Science Foundation under grants CNS-0721744 and DBI-0529012. The work of Huang was also partially supported by the National High Technology R&D Program (863 Program) of China under 2006AA01A114 and the work of Fang was also partially supported by the 111 Project under B08038 with Xidian University, Xi'an, China.

X. Huang is with the Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, Shenzhen, China (e-mail: xx.huang@sub.siat.ac.cn).

H. Zhai is with Philips Research North America, Briarcliff Manor, NY (e-mail: hong.zhai@philips.com).

Y. Fang is with the Department of Electrical and Computer Engineering, University of Florida (e-mail: fang@ece.ufl.edu). He is also holding the Changjiang Scholar Chair Professorship with the National Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, China.

Digital Object Identifier 10.1109/T-WC.2008.060680

The broadcast nature of wireless medium has been exploited widely in literature. Without additional transmissions, nodes inside the transmission range of a sender are able to obtain a copy of the packet forwarded to an intended receiver. Dense wireless sensor networks offer the opportunity to develop novel communication and routing techniques based on cooperation among nodes in the neighborhood. The failure probability of all links is much smaller than that of a single link. Although there are many previous studies on cooperative communication and routing, most of them focus on physical layer design. Robust routing against path breakage still remains unexplored. Our main contribution is the investigation of distributed energy efficient robust routing catering to mobile wireless sensor networks. In our proposed protocol, cooperative relay is performed at each hop, so only local knowledge is necessary. Multi-node cooperation involves lower layer coordination. Our robust cooperative routing is based on cross-layer design with MAC layer as the anchor, operated under IEEE 802.11 MAC protocol, which has been proven effective in our prior work [1].

After establishing a path between source and destination nodes, robust cooperative routing is able to provide reliable packet delivery against both temporary and permanent path breakage. If a node moves away, the resulting path breakage is permanent. Interference and fading may cause temporary path failure. As a distributed approach, robust routing is relieved from the substantial control overhead for route maintenance, update and repair. Only 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 for routing. Choosing reliable links potentially reduces retransmissions, thus saving energy and shortening delay. Our analysis shows that cooperative routing outperforms non-cooperative routing in terms of energy efficiency when link error probability or node mobility is high. Simulation result confirms that our robust cooperative routing protocol improves performance significantly 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 illustrates the robust cooperative routing scheme. The reliability and energy efficiency of cooperative and non-cooperative routing without overhearing are evaluated and compared analytically in Section IV. Section V demonstrates and discusses the simulation results. Section VI concludes the paper.

II. Related Work

Many papers explore the cooperative diversity to combat fading channels [2]-[8] by allowing multiple nodes to transmit

simultaneously. In [9], Kwon et al. propose a routing strategy to minimize the energy consumption for packet delivery constrained by reliability requriement, then choose the corresponding optimal transmission power and the retransmission limit. ExOR [10] is proposed to increase the throughput in multi-hop wireless networks to take advantage of multiple forwarders. In [11], a modified version of AODV over specialized IEEE 802.11 MAC protocol is proposed to strengthen the path reliability through selecting the optimal relay node. Combining a MAC protocol capable of channel-state based next hop selection [12] with AOMDV [26], the proposed method could deal with packet loss due to channel error. Zhu and Cao [13] utilize multi-hop relay at MAC layer to achieve higher throughput given multi-rate physical links. Assuming nodes are rational, Srinivasan et al. [14] apply game theory to the problem of cooperation of energy constrained nodes. The authors in [15] work on the cross-layer design in which a set of cooperating nodes are selected to transmit to a set of receiving nodes 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 design. We extend our previous work [16] and analyze the performance in terms of robustness and energy efficiency.

Cooperative caching, sharing and coordination of cached data among multiple nodes can improve the delay and reliability of packet delivery in wireless ad hoc networks. Yin and Cao propose cooperative data, path and hybrid caching [17] to reduce the query delay and message complexity. In [18], the authors employ cooperative packet caching and shortest multipath routing to reduce packet loss due to frequent route failure and end-to-end delay.

In a 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 to mobile wireless sensor networks. DSDV [19], AODV [20], DSR [21], ZRP [22] are the most well known routing protocols for mobile ad hoc networks. Many follow-on works are proposed to further improve the performance [23]-[27]. It is shown that path diversity can be utilized to improve the maximum channel loss of the route significantly [28].

III. Robust Cooperative Routing Protocol (RRP)

Due to the broadcast nature of wireless medium, neighboring nodes of a transmitting node can overhear the packet, which is called *Wireless Broadcast Advantage (WBA)* [29]. This is illustrated in Fig. 1. Inherently, it is also cooperative caching in the neighborhood. As nearby nodes with a copy serve as caches, the next-hop node could retrieve the packet from any of them. Suppose node 1 attempts to deliver a packet to node 5 over path $1-3-5$. When 1 transmits to node 3, nodes 2 and 6 may also correctly receive the packet. Cooperation among those nodes may result in high energy-efficiency and robustness when we carefully utilize diversity.

In our work, we assume the wireless sensor network is densely deployed, so each node has plenty of neighbors. In our proposed robust cooperative routing protocol (RRP), multiple

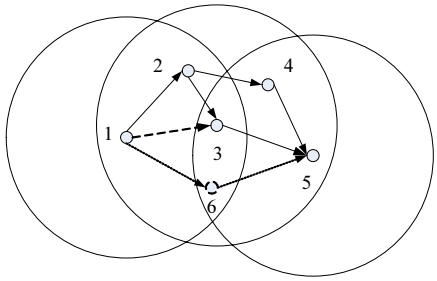


Fig. 1. Relay path with equivalent or remedy nodes.

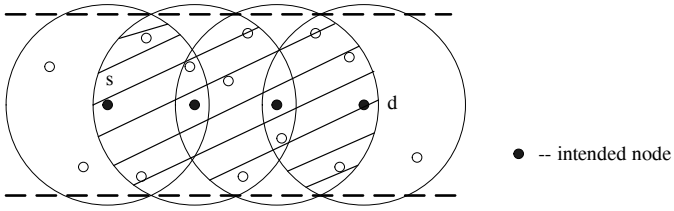


Fig. 2. A robust path between s and d.

nodes with a same packet attempt to deliver it to another node cooperatively. Assume all nodes have the same transmission range and a path has already been established between a source and a destination, which is referred to as the intended path. The nodes on the intended path are called intended nodes. A guard node is at least a neighboring node of two intended nodes, i.e., a guard node can reach at least two intended nodes. Likewise, a link between a guard node and an intended node is called a guard link. As guard nodes are able to take advantage of WBA, they can work cooperatively to deliver packets along the intended path. The intended path, along with the guard nodes, collectively constitute the *robust path* (the wider path), which is used to enhance the robustness. Thus, using multiple guard links, the robustness of an intended link is enhanced at each hop. Revisit the example in Fig. 1, if link $1-3$ fails due to deep fading or the departure of node 3, then node 3 cannot receive the packet correctly. Without waiting for potential multiple retransmissions over the unreliable or disappeared link $1-3$ before re-routing or dropping the packet, a substitute link $2-4$ or $6-5$ could transfer the packet proactively. As long as at least one link is capable of delivering the packet successfully, the packet can be received and further forwarded towards the destination. Actually, robust routing works like forwarding in a zone. Nodes in the zone collaboratively forward the packet to the next zone progressively towards the destination. Different from the traditional narrow path consisting of one node at each hop, the robust 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 successfully receiving the packet will help forward the packet proactively to the downstream node(s) without waiting for the routing instruction (re-routing via alternate path). The packet is delivered to the intended downstream node (the two-hop-away node on the path) if reachable, or to the node that lost the packet otherwise.Fig. 1 best illustrates the idea. Through node 6, the

number of transmissions needed from node 1 to node 5 reduces to 2 if node 6 transfers the packet successfully. Otherwise, the total number of transmissions needed from node 1 to 5 would be at least 4, if node 1 only retransmits to node 3 once and selects another path, say $1-6-5$, 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 can improve the reliability and reduce the end-to-end delay at the cost of spending more energy in overhearing at guard nodes. On the other hand, energy savings via avoiding retransmissions over a hostile or lost link may potentially offset the energy consumption of overhearing. It is possible that cooperation among guard nodes lowers the energy consumption while achieving robustness. Finally, our approach is different from traditional relaying and alternative routing. Traditional relaying schemes forward the overheard packet to the intended receiver of the packet transmission while our RRP forwards packets to reachable downstream nodes closer to the destination. Traditional alternative routing has to wait for the time-out at the network layer (i.e., after multiple retransmission attempts at the MAC layer and declaring the link failure) and then find the alternative path to replace the failed path while our RRP could forward the packet at the MAC layer, hence reduces the transfer delay at the intermediate nodes on the path. Rather than purely relying on the network layer to implement cooperation, MAC and network layer cooperation can achieve better channel utilization, reduce delay and improve energy efficiency. Our RRP is different from multicast or anycast, because cooperation nodes have the knowledge about succeeding nodes. So the trace of a packet is restricted in the determined robust path, instead of propagating information network-wide.

A. Robustness Against Node Mobility

From the previous discussion, it is obvious that our RRP is distributed. Cooperative nodes just need local information and partial knowledge about the intended path. This features another advantage of cooperative routing – rapidly adaptive to the changing topology.

As a node on the original path moves, the set of guard nodes changes accordingly. So the effective guard node set is also dynamic in mobile wireless networks. The dynamic change comes from two scenarios. One is due to the movement of intended nodes. The other is the mobility of guard nodes themselves. When a guard node moves out of the range of the robust path, it automatically quits its role in the cooperative routing as it cannot hear the communication over the intended path any more. If a node moves into the communication range of a path, it learns the partial path information by overhearing ongoing transmissions. It decides its role in routing based on the information in the decoded overheard packet header. If it hears transmissions correctly from two intended nodes that belong to the same flow, indicated by the source and destination nodes, it determines itself qualified to be a relay node. When many nodes on the intended path move away, a new path has to be established in conventional routing algorithms. However, through cooperative routing within the robust path, a new path is automatically set up with minor overhead. It is unlikely that all nodes in the robust path move out at a hop and cause failure of the zone during a packet delivery. Thus, our robust cooperative routing RRP is applicable to highly dynamic wireless sensor networks.

B. Robust Path Formation

After an intended path is established between a source-destination pair, every node on the path broadcasts partial path information to help construct the robust path. According to the definition, the robust path consists of nodes on the intended path and the corresponding guards nodes. Now we need to identify guard nodes through the broadcast information. The broadcast information includes source node, destination node, node ID of the current node, its upstream and downstream nodes. We will explain later how to use this information. The source and destination nodes are used to identify an intended path. If a node hears a packet, either control or data packet, from two different nodes belonging to the same intended path, it is eligible to participate in the cooperative routing and becomes a guard node. Among the intended nodes within the transmission range of the guard node, the one 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 for packet forwarding. If a node belongs to several robust paths, it maintains a record for each path. Details about the robust path is illustrated in the next subsection.

An example of building up a robust path is shown in Fig. 2. The shaded area shows the robust path formed between s and d. Guard nodes must reside in the robust path. As all nodes over the robust path have partial knowledge about the intended path, the cooperation among them would improve responsiveness to path failure because they can use the available information to recover from the failure.

C. Cooperation Among Guard Nodes

Based on the relative location to the intended node, guard nodes can be classified into two categories and behave differently. The most preferred guard node can substitute an intended node if it is the neighbor of a pair of two-hop away intended nodes. When the replaceable intended node fails to relay the packet, the packet is blocked and goes through the guard node, then back to the intended path. Since this kind of nodes acts as the backup nodes of the intended path, this kind of nodes is called equivalent nodes. Denote N_e the set of equivalent nodes.

Our MAC layer protocol is a modified version of IEEE 802.11 MAC and the RTS/CTS handshake works the same way as in IEEE 802.11. After finishing data transmission, the sender waits for an ACK. If the intended receiver successfully receives the packet, it replies with an ACK after Short Inter-Frame Spacing (SIFS). Otherwise, the channel is silent during this interval. A guard node learns that the intended link fails and replies an ACK to the sender and then relay 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

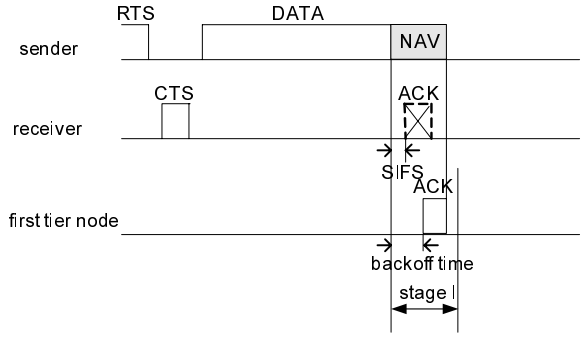


Fig. 3. A first tier node is a relay node.

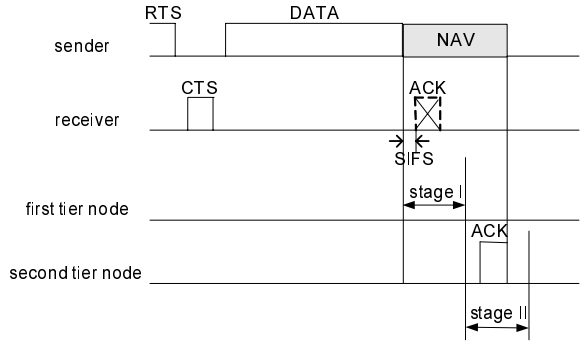


Fig. 4. A second tier node is a relay node.

after a successful reception, the node eligible to help relay can reply an ACK. The first replying node will be the relay node. Since the carrier sensing range is normally larger than twice of the transmission range, for example, default carrier sensing range is 2.2 times the transmission range in the simulator NS-2, the ACK can be heard or sensed by all other guard nodes.

It is possible that several nodes are equivalent nodes. To break the tie and reduce potential collisions, equivalent nodes respond to the sender after backoff time, say $T_{boe,m}$. The backoff time 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 timer hear or sense the ACK, they stop competing for relay. Thereafter, election for the relay node finishes. The backoff delay is given in (1).

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

where

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

and T_e is the backoff window for equivalent nodes. P_m is a mixed metric of normalized link delay D_m and the error probability E_m of the link between node m and the downstream node of the failed intended node. To better adapt to mobile environment, V_m which is the relative mobility to the intended downstream node, is considered in coordination. Ranging from [0.01, 1], V_m is the normalized average relative moving speed. If zero is an allowed value, multiple stationary nodes will wait for the same backoff time SIFS, and cause collision. So the relative mobility is normalized to fall into the interval of [0.01, 1]. V_m is used as a prediction of stability. A highly mobile node results in an unstable link. A node with zero or low relative mobility is preferred as it is less likely to cause link breakage during a transmission. Reliability E_m is an indication of 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, longer link delay is expected. With these two factors, a link with less contention and higher reliability tends to be selected as the relay node. 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 is available. Now, the second tier nodes are allowed to compete for relaying. The second tier, referred to as remedy nodes, contains the common neighbors of an intended node and its downstream node, or neighbors of both an intended node and an equivalent node. 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 always have lower priority to relay than equivalent nodes. The second competition stage begins if no equivalent node transmits in the first stage. 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 the case for equivalent nodes, they defer with backoff time

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

where T_r is the backoff window for remedy nodes. Any guard node hearing or sensing an ACK from another guard node assumes that a successful cooperation is completed. So it just discards the received packet. The maximum backoff time for remedy nodes is $SIFS + T_e + T_r$. The time interval between DATA 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. 4. The shortcoming of judging a successful relay through sensing is that a guard node probably drops a packet by mistake. When the received power is too weak to decode the packet, it is not able to determine the sender of the packet. If the packet is from a node that is not a cooperation node, it still regards it as an ACK from another qualified relaying node. Then it assumes a more qualified node will relay the packet and quits cooperation. Robust routing RRP fails if all relaying nodes sense a packet from a non-relaying node before the backoff timers of all guard nodes reach zero, then the sender will retransmit. However, the probability of this case is generally low in mobile wireless sensor networks with moderate traffic load.

If an intended node continuously fails to receive correctly for T_p packets consecutively, it is assumed to be away from the intended path or a failed node. In both cases, it no longer qualifies for routing. The guard node recently accomplishing the forwarding will then substitute the failed node, and become the new intended node by broadcasting the same information as in the robust path formation phase. Then new sets of equivalent nodes and remedy nodes will be constructed

accordingly. In this case, former guard nodes which become outside of the transmission range of the new intended node will not be aware of the path recovery process. They discard all information about the outdated intended path and quit routing after timeout.

The backoff time for each guard node is unpredictable, but the maximum backoff time or competition interval is controllable. If a 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). All nodes set NAV as the sum of the NAVs in IEEE 802.11, $NAV_{802.11}$ and the maximum backoff time T_{max} for cooperation, written 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 other transmissions. The shortcoming of using the new NAV value is that even if an ACK is sent back to the sender before NAV goes to zero, nodes are still idle for the rest of NAV. However, T_{max}, which is on the order of several hundred microsecond, is much smaller than the time for retransmission (usually on the order of millisecond for 1K data packets). Our RRP still has a shorter delay than the conventional retransmission schemes. The value of T_{max} depends on the network density. If the density is high, potentially more nodes are eligible for cooperative routing. Therefore, T_{max} should be large enough to reduce the probability of ACK collision among relaying nodes.

IV. Performance Analysis: Analytical Results

Based on some reasonable assumptions, we compare the energy efficiency of our cooperative routing RRP and traditional routing. First we need to find the average number of guard nodes. We compute the two sets of guard nodes separately. Assume nodes are uniformly distributed with a density of D. The path from a source to a destination is $n_0, n_1, ..., n_h$, where $n_0 = s$, $n_h = d$. Denote $d_{i,j}$ the distance between node i and j. The transmission range of each node is R and the energy consumption for a transmission is E_t. The shaded area in Fig. 5 shows where equivalent nodes are probably present. Apparently, $R < d_{i-1,i+1} \le d_{i-1,i} + d_{i,i+1}$. The area of the shaded region at node i, denoted as $S_e(i)$, is

$$\begin{aligned} S_e(i) &= 2\left(\frac{\angle AiB}{2\pi}\pi R^2 - \frac{d_{i-1,i+1}}{2}\sqrt{R^2 - \left(\frac{d_{i-1,i+1}}{2}\right)^2}\right) \\ &= 2R^2 \arccos\left(\frac{d_{i-1,i+1}}{2R}\right) - d_{i-1,i+1}\sqrt{R^2 - \left(\frac{d_{i-1,i+1}}{2}\right)^2} \end{aligned} \tag{3}$$

The average number of equivalent nodes $N_e(i)$ is

$$\begin{aligned} N_e(i) &= S_e(i)\cdot D - 1 = 2DR^2 \arccos\left(\frac{d_{i-1,i+1}}{2R}\right) - \\ & Dd_{i-1,i+1}\sqrt{R^2 - \left(\frac{d_{i-1,i+1}}{2}\right)^2} - 1 \end{aligned} \tag{4}$$

The shaded area in Fig. 6 indicates the region of remedy nodes located in. Similar to (3), the overlapping transmission area of node $i-1$ and i is

$$S_{overlap}(i) = 2R^2 \arccos\left(\frac{d_{i-1,i}}{2R}\right) - d_{i-1,i}\sqrt{R^2 - \left(\frac{d_{i-1,i}}{2}\right)^2} \tag{5}$$

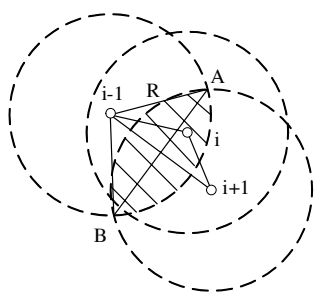


Fig. 5. Region of equivalent nodes.

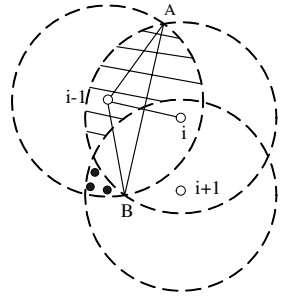


Fig. 6. Region of remedy nodes.

The area covered by the equivalent node but beyond the coverage of remedy nodes, indicated by the dotted region in Fig. 6, is negligible. So the area of the remedy nodes at node i, denoted as $S_r(i)$, between node $i-1$ and i is approximately

$$S_r(i) \ge S_{overlap}(i) - S_e(i) \tag{6}$$

The lower bound of the average number of remedy nodes between node $i-1$ and node i, denoted as $N_r(i)$, is

$$N_r(i) = S_r(i)\cdot D - 2 \tag{7}$$

For simplicity, we assume that the link error probability, say p, is the same for all links between all nodes in the robust path. So the success probability of a single transmission is $P^e_{succ} = 1 - p^{N_e+1}$.

Denote E_r the energy consumption in reception. The probability that k out of N_e+1 nodes receive the packet is actually binomially distributed. So the total energy consumption E_k and the probability of k successful receptions P_k are

$$E_k = (E_t + kE_r), \quad P_k = \begin{pmatrix} k \\ N_e+1 \end{pmatrix} p^{N_e+1-k}(1-p)^k$$

respectively. So the expected energy consumption for a successful transmission from node $i-1$ without retransmission, denoted by C^e_1, is

$$\begin{aligned} C^e_1 &= \sum_{k=1}^{N_e+1} E_k P_k P(k \ge 1) \\ &= \frac{1}{1-p^{N_e+1}} \sum_{k=1}^{N_e+1} \begin{pmatrix} k \\ N_e+1 \end{pmatrix} p^{N_e+1-k}(1-p)^k (E_t + kE_r)_k \\ &= E_t + E_r \frac{(N_e+1)(1-p)}{1-p^{N_e+1}} \end{aligned}$$

Ideally, we assume that a node retransmits for infinite times. So the expected energy consumption for a successful delivery from node $i-1$ to equivalent nodes or node i is

$$C^e = \sum_{l=0}^{\infty} (C^e_1 + lE_t)(1-P_{succ})^l P_{succ} = C^e_1 + E_t \frac{1-P_{succ}}{P_{succ}} \tag{8}$$

Substituting C^e_1 and P^e_{succ} into C^e,

$$\begin{aligned} C^e &= E_t + E_r \frac{(N_e+1)(1-p)}{1-p^{N_e+1}} + E_t \frac{p^{N_e+1}}{1-p^{N_e+1}} \\ &= E_r \frac{(N_e+1)(1-p)}{1-p^{N_e+1}} + E_t \frac{1}{1-p^{N_e+1}} \end{aligned} \tag{9}$$

Now we calculate the expected energy consumption of a successful delivery from node $i-1$ to i of non-cooperative

routing, denoted as C_{nc}, is

$$\begin{aligned} C_{nc} &= E_s N_e + E_r + (1-p)E_t + p(1-p)2E_t + \cdots \\ &= E_r + \sum_{l=1}^{\infty} p^{l-1}(1-p)lE_t = E_s N_e + E_r + \frac{E_t}{1-p} \end{aligned} \tag{10}$$

Experiment [30] shows that the energy consumption ratio for idle:receive:transmit is 1:1.05:1.4. So a node consumes nearly the same amount of energy in carrier sensing (idle) as in reception. Therefore, (10) can be rewritten as

$$C_{nc} = E_r(N_e + 1) + \frac{E_t}{1-p} \tag{11}$$

Since $0 \le p \le 1$,

$$\frac{E_t}{1-p^{N_e+1}} \le \frac{E_t}{1-p}, \quad E_r\frac{(N_e+1)(1-p)}{1-p^{N_e+1}} \le E_r(N_e+1)$$

Thus,

$$C^e \le C_{nc}$$

Even our assumption de-emphasizes the cooperative diversity due to the assumption of identical link error probability, the energy efficiency of cooperative routing still outperforms non-cooperative routing. Therefore, it is preferable to apply cooperative routing in unreliable mobile wireless sensor networks.

When there are no equivalent nodes but only remedy nodes, the number of retransmissions from node $i-1$ to i in RRP is bounded by the number of retransmissions in non-cooperative routing. As we mentioned earlier, the assumption of identical link error probability de-emphasizes the efficiency of diversity. When the link error probability is different for different links, which is the case in many practical situations, RRP tends to utilize the most reliable link, resulting in fewer number of retransmissions, and still achieves relatively good performance.

When the intended node i leaves, the link fails, so the link error probability is 1. In this situation, non-cooperative routing will retransmit until reaching the maximum number of attempts to declare the link failure. Suppose links to or from the intended node i have higher error probability, say p_i, than other links which have the same error probability p. In cooperative routing, a packet goes through a remedy node to the next-hop remedy node, then back to the intended path at the intended downstream node. Since the most separated pair in the two succeeding sets of remedy nodes may be farther than one-hop, we assume that a remedy node can only reach one next-hop remedy node. The probability that a transmission is successful for cooperative routing is

$$P^r_{succ} = 1 - p + p^{N_e+1}(1-p^{N_r})(1-p),$$

while for non-cooperative routing is

$$P^{nc}_{succ} = 1 - p_i$$

Apparently, $P^r_{succ} > P^{nc}_{succ}$.

Similar to the calculation for equivalent nodes, the expected energy expenditure C^r_1 is

$$C^r_1 = 2E_t + E_r\frac{N_r(1-p)}{1-p^{N_r}} + E_r \tag{12}$$

When remedy nodes relay a packet, the packet has to traverse two hops to detour the failed intended node. Similar to (8), the expected energy consumption in cooperative routing via remedy nodes is approximately

$$\begin{aligned} C^r &= 2E_t + E_r\frac{N_r(1-p)}{1-p^{N_r}} + E_r + E_t\frac{p-p^{N_e+1}(1-p^{N_r})(1-p)}{1-p+p^{N_e+1}(1-p^{N_r})(1-p)} \\ &= E_r(\frac{N_r(1-p)}{1-p^{N_r}} + 1) + E_t(1 + \frac{1}{1-p+p^{N_e+1}(1-p^{N_r})(1-p)}) \end{aligned} \tag{13}$$

Comparing to $C_{nc} = E_r(N_r+1) + \frac{E_t}{1-p}$,

$$E_r(\frac{N_r(1-p)}{1-p^{N_r}} + 1) \le E_r(N_r+1)$$

As $p \to 1$,

$$E_t(1 + \frac{1}{1-p+p^{N_e+1}(1-p^{N_r})(1-p)}) \le \frac{E_t}{1-p}$$

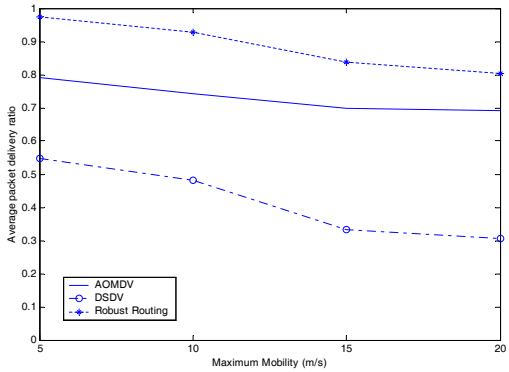
Therefore, using remedy nodes, RRP can still save energy when the link error probability is high.

V. Performance Analysis: Simulation Results

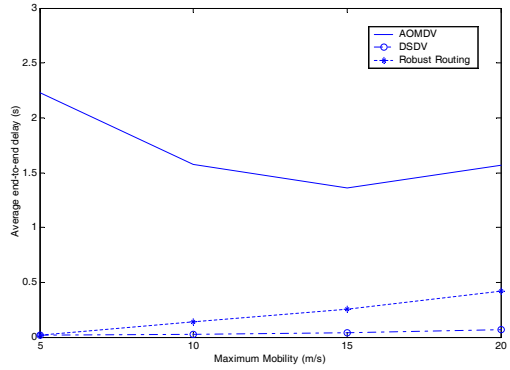
In this section, we present simulation results of our scheme RRP along with DSDV and AOMDV in NS-2. AOMDV establishes multiple alternative paths during the path establishment stage. In the comparison, we use three paths for each source-destination pair in AOMDV. We use two-ray ground model as the physical propagation model to the study the performance of the three routing protocols in outdoor environment. 15 nodes are randomly distributed in a $600m \times 600m$ field. Two flows are randomly generated. The source generates packets at a rate of 20packets/s with size of 1000 bytes. Every node moves according to the random waypoint mobility model. The minimum speed of nodes is 1m/s and the maximum speed of each node changes from 5m/s to 20m/s to investigate the performance with respect to node mobility. A simulation lasts for 600 seconds. We measure the packet delivery ratio, the end-to-end packet delay, and the energy consumption per bit. The energy consumption per bit is the energy cost of sending a bit from the source to the destination.

Fig. 7(a) 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. 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.

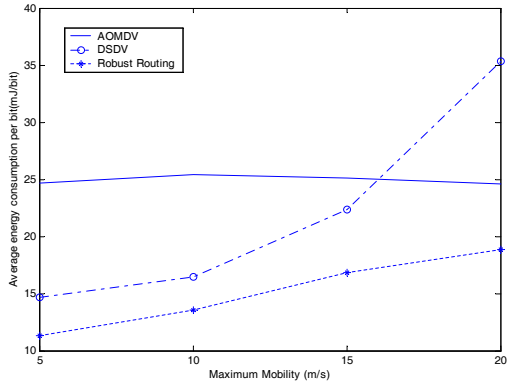
Robust routing performs better than AOMDV, but a little inferior to DSDV in terms of end-to-end delay, as shown in Fig. 7(b). As a proactive routing protocol, routing information is stored at each intermediate node before packet arrival in DSDV. Therefore, packets are immediately forwarded upon reception. However, AOMDV is an on-demand routing protocol. A packet has to wait until paths are found, so it tends to experience longer delay. Our robust routing protocol



(a) Packet delivery ratio

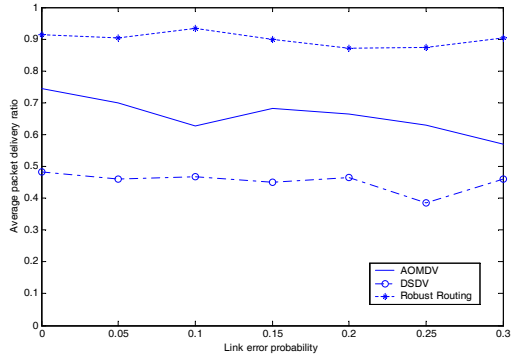


(b) End-to-end delay

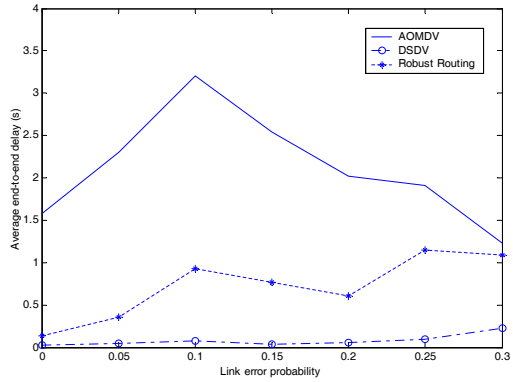


(c) Energy consumption

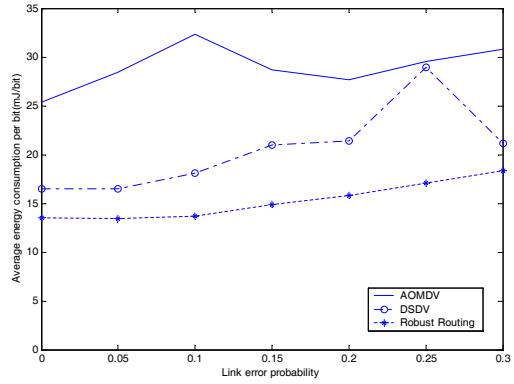
Fig. 7. Effect of node mobility.



(a) Packet delivery ratio



(b) End-to-end delay



(c) Energy consumption

Fig. 8. Effect of link error rate at maximum mobility 10m/s.

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.

Observe in Fig. 7(c), the energy consumption per bit of our robust routing protocol increases as the node mobility increases. The energy consumption of AOMDV is loosely correlated with node mobility because incurred control overhead during path discovery does not change much with node mobility. As expected, the energy consumption of DSDV increases sharply with node mobility because frequent topology changes incur heavier overhead. Our robust routing protocol also consumes more energy as node mobility increases, but at a much lower rate than DSDV. It selects the best relay node with moderate message exchange instead of establishing a new end-to-end path. The energy consumption of RRP is lower than that of AOMDV at relatively low mobility, but slowly grows close to it as the maximum node mobility increases. The reason is that packets have to go through the cooperation process frequently at high mobility. Also, the update messages are sent out more frequently by the newly self-nominated node on the intended path to refresh path information, which accounts for the rise in energy consumption.

Link error probability is also a significant factor which impacts the performance of routing protocols, so we measure

those performance metrics subject to various link error probability as well. Due to the page limit, only the performance under maximum node mobility of 10m/s is shown. As the link error probability increases from 0 to 0.3, the packet delivery ratio drops as expected. However, our scheme is relatively immune to link error. As shown in Fig. 8(a), the packet delivery ratio of robust routing decreases slightly, while that of DSDV and AOMDV drops substantially. Again, Fig. 8(b) demonstrates that DSDV achieves the best end-to-end delay, followed by robust routing and then AOMDV. As expected, the end-to-end delay of robust routing increases with the link error probability because of the longer latency for selecting an available path and more retransmissions. RRP delivers packets with longer delay than DSDV because of the longer backoff delay and the cooperation procedure. Instead of relying on retransmissions at MAC layer and searching for new paths, RRP delivers the packet over the most reliable path located in the robust path. RRP is the most energy efficient as shown in Fig.8(c). The underlying reason is that our protocol only carries out path repair in a restricted region, while AOMDV and DSDV invoke network wide path recovery. Cross-layer design contributes to the performance gain of RRP. This justifies the application of RRP in energy constrained mobile wireless sensor networks.

VI. Conclusion

This paper presents a cross-layer robust routing protocol based on node cooperation among nearby nodes for unreliable mobile wireless sensor networks. Inside the robust path expanded from an intended path, a reliable path is selected for packet delivery. Based on the path quality, the intended path is able to adapt to the varying topology. Utilizing path diversity in the robust path, the robust routing protocol is capable of selecting the best path in a wide zone for each packet. This is the difference of our RRP from traditional routing protocols. Therefore, the robustness against path breakage is improved.

References

[1] H. Zhai, X. Chen, and Y. Fang, "Improving transport layer performance in Multihop ad hoc networks by exploiting MAC layer information," *IEEE Trans. Wireless Commun.*, vol. 6, no. 5, pp. 1692-1701, May 2007.

[2] B. S-Mergen and A. Scaglione, "A continuum approach to dense wireless networks with cooperation," in *Proc. IEEE INFOCOM 2005*, vol. 4, pp. 2755-2763, Miami, FL, Mar. 2005.

[3] 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.

[4] L. Liu and H. Ge, "Space-time coding for wireless sensor networks with cooperative routing diversity," in *Proc. Asilomar Conf. on Signals, Systems and Computers 2004*, vol. 1, pp. 1271-1275, Nov. 2004.

[5] 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.

[6] 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.

[7] 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.

[8] Y. Zhu and H. Zheng, "Understanding the impact of interference on collaborative relays," *IEEE Trans. Mobile Computing*, vol. 7, no. 6, pp. 724-736, Jun.e 2008.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] H. Zhu and G. Cao, "rDCF: a relay-enabled medium access control protocol for wireless ad hoc networks," in *Proc. IEEE INFOCOM 2005*, vol. 1, pp. 12-22, Miami, FL, Mar. 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] 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.

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

[17] 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.

[18] A. C. Valera, W. K. G. Seah, and S. V. Rao, "Improving protocol robustness in ad hoc networks through cooperative packet caching and shortest multipath routing," *IEEE Trans. Mobile Computing*, vol. 4, no. 5, Sept./Oct. 2005.

[19] 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.

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

[21] D. B Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Computing*, vol. 353, pp. 153-181, 1996.

[22] Z. J. Haas, "A new routing protocol for the reconfigurable wireless networks," in *Proc. IEEE Int'l Conf. on Universal Personal Commun.*, pp. 562-566, Oct. 1997.

[23] O. H. Hussein, T. N. Saadawi, and M. J. Lee, "Probability routing algorithm for mobile ad hoc networks' resources management," *IEEE J. Select. Areas Commun.*, vol. 23, no. 12, pp. 2248-2259, Dec. 2005.

[24] S. J. Lee and M. Gerla, "AODV-BR: backup routing in ad hoc networks," in *Proc. IEEE WNMC*, vol. 3, pp. 1311-1316, Sept. 2000.

[25] H. Chen and C. Lee, "Two hops backup routing protocol in mobile ad hoc networks," in *Proc. Int'l conf. on Parallel and Distributed Systems*, vol. 2, pp. 600-604, July 2005.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] M. Stemm and R. H. Katz, "Measuring and reducing energy consumption of network interfaces in hand-held devices," *IEICE Trans. Commun.*, vol. E80-B, no. 8, pp.1125-1131, Aug. 1997.