Spatially Diffuse Pathsets for Robust Routing in Ad Hoc Networks

Trisha Biswas, Rudra Dutta
North Carolina State University
Email: (tbiswas, rdutta)@ncsu.edu

***Abstract*—Ad hoc wireless networks are characterized by frequent node mobility, limited power reserves and interfering transmissions. On-demand routing proves to be more successful in such networks, as it reduces the traffic overhead of sending periodic updates, but they may be susceptible to both random uncertainty in radio links, and malicious jamming. We consider a network of nodes addressed by their locations, and propose a novel routing technique that we call Petal Routing, which maximizes reliability by using pathsets, made of diverse multiple paths, in place of a single path. Petal Routing takes advantage of the broadcast nature of wireless networks to reduce the number of transmissions for multiple paths by overlapping the multiple diverse paths. Various tunable parameters built into the approach can be used to improve metrics such as delay, number of transmissions and packet delivery ratio. We evaluate the performance of our scheme using extensive simulations, and show that it is viable.**

I. Introduction

Ad hoc wireless networks have many desirable features, notably their ability to be deployed and be operational nearly instantly, making for their suitability in applications such as tactical networks. They also have their unique challenges, one of which is the difficulty in guarding against failures of path transmissions due to the inherent uncertainty and vulnerability of the wireless medium. Such failures may be random, or actively caused by malicious opponents, i.e. jamming. In networking literature, techniques to ensure network continuity have been well investigated, and can be categorized into proactive and reactive measures, or combinations of both. For tactical networks, some degree of proactivity is desirable, to prevent the loss of critical messages, or the long delay involved in detecting a loss and retransmitting. However, proactive measures typically involve redundant transmissions, which reduce the efficiency of utilizing the transmission medium, made worse in the wireless medium because of the limitations on simultaneous transmissions posed by wireless interference. Thus a tradeoff exists between reliability and overhead. For a practical application, not all messages are likely to be equally critical. In such a case, a network which wastes resources to provide very high reliability for all messages proactively (even when there are no jammers) may be as bad as a network which provides no reliability. The goal of our research in this paper is to provide a proactive algorithm which allows a sender to specify a relative degree of desired reliability *a priori*, while admitting of a reactive use of the same mechanism to step up the target reliability when network conditions so indicate.

To this end, we investigate using multiple paths to introduce redundancy and therefore increase reliability in such networks. Multipath routing has been proposed before to increase reliability in wired and wireless networks. The information to be transmitted along the multiple paths can be complete replications of the desired message, or partial/combined versions to reduce overhead; this latter is the approach taken by network coding. We base our approach on complete replications; this allows us to take a different approach to reducing overhead - that of *spatially diffuse pathsets*. Such a pathset is defined as a contiguous area including the source and destination nodes, inhabited by other nodes. The message spreads as a flow through this area, and travels to the destination by one or more paths. The extent of this area can be used as a parameter to target a desired level of reliability. Since the area is contiguous, various nodes can overhear each other, and this allows them to cancel transmissions which are known to be redundant, reducing overhead. Since there is always an uncertainty in such decisions, they can be parameterized to provide further mechanisms for meeting the target reliability. Our approach can be considered a form of restricted flooding, which has the desirable characteristic that nodes do not have to maintain neighborhood information or end-to-end paths.

In this paper, we focus on defining the mechanism and the parameters for this approach. We do not here address establishing an analytical relationship between these parameters and desired levels of reliability, or allowing the target level to be expressed in practical terms; this is part of our ongoing work. We measure the effect of our approach simply by the mathematical definition of reliability; for a given message transmission from source to destination, the *reliability* is a mission-specific metric: the probability that the message will reach its destination.

II. Related Work

Multipath routing in wireless networks has been addressed in literature [1] in broadly two categories: (a) sending redundant information using multiple paths [2], [3], and (b) maintaining one or more alternate paths for back-up [4], [5]. Some multipath techniques are extensions of single path routing schemes [6] and use the latter to find a set of end-to-end paths. Reliability of transmissions can be increased [7] with multipath routing in presence of network failures. However, the discovery and maintenance of multiple paths increases control overhead [8]. Location aided routing (LAR) [9] involves using geographic location to carry out routing. LAR or geographic routing techniques have been used to reduce message flooding in single path routing schemes [10] (e.g. beacon messages).

This work is supported by the U.S. Army Research Office (ARO) under grant W911NF-08-1-0105 managed by NCSU Secure Open Systems Initiative (SOSI). The contents of this paper do not necessarily reflect the position or the policies of the U.S. Government.

978-1-4244-9268-8/11/$26.00 ©2011 IEEE

Other approaches include SDAR [11] where the goal is to guarantee security and annonimity of transmissions. ExOR [12] uses node broadcasts where intermediate nodes communicate with one another to decide on the node that would carry the packet forward. Our approach uses geographic routing to compute a spatially diffuse pathset to increase reliability of transmissions.

III. Towards robust multipath routing

In this section we discuss the assumptions and failure models used in our routing scheme. Our technique utilizes the broadcast nature of wireless networks to combine multiple transmissions from one node to one transmission [1]. The basic idea is as follows. Given a source and destination, the network carries out *constrained flooding* to send the packet to the receiver. The flooding is constrained to transmissions within an area that we call a *spatially diffuse pathset*, or more intuitively as a "petal" (Fig. 1), because of the shape, the two ends of which converge at the source and destination. This is the general description of a petal; to apply this concept, some specific shape schema must be used, we provide an example later. This technique also allows for further enhancements to reduce the number of transmissions within the diffuse pathsets. Since the underlying protocol is flooding, the individual nodes do not need any prior information about their neighbors or maintain any end-to-end paths.

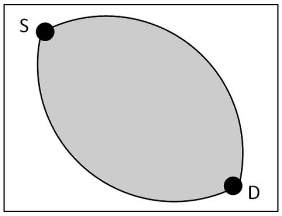

Fig. 1. Diffused overlapping pathsets

A. Assumptions

As in other geographic routing techniques [10], our scheme uses locations to uniquely identify nodes. Messages are routed to the location of the destination instead of a network address. It is assumed that a node always knows its current location. This is a common assumption in georouting techniques [10]. In addition to that, the source knows the location of the destination. The (x, y) coordinate of a node is in the form: $(longitude, latitude)$. The nodes in the network need not maintain routes to any other node in the network, or know who their neighbors are. This allows us to model cases where the location *is* the address, i.e. a message is desired to travel to a particular location, rather than an identified node. For other cases, this approach is compatible with any other type of node identifiers, with an appropriate mapping service; we do not consider this in the scope of our work.

We assume that the network is reasonably dense. If no path exists within the flooding area, then the routing would naturally fail; if only a single path exists, then a multipath approach is not appropriate. However, in case of a sparsely populated network, our approach could still be used in combination with table-driven approaches to store neighbor information, which can assist in calculating the optimal area for flooding, i.e. the "width" of the petal as we discuss later. We assume that nodes are aware of the average node density in the network; a reasonable assumption since it depends only on network span and number of nodes. The distribution of node density information to the network nodes is considered outside the scope of this paper.

In a densely populated wireless network, collisions are an important concern that can lead to poor performance. MAC layer algorithms for contention resolution in wireless networks have been studied extensively, e.g. [13]. Moreover, the multihop path occurs through a time scale that is more coarse grained, and it does not affect the overall end-to-end performance. We assume that the contention resolution and scheduling issues at the hop time scale are handled by the MAC layer. In the network layer, we provide some heuristic enhancements using back-off time and redundancy tuning, to reduce the probability of collisions.

We assume low mobility in the network, so that the destination location does not change significantly over the timescale of the transmission of messages from source to destination. To allow for minor movement of nodes, we consider the destination to be within a small radius of its most updated location that the source has. The mobility of intermediate nodes is not of particular concern, because the location of a node at an instant it receives a transmission determines whether or not it is part of the diffuse pathset. No pre-determined assumptions are made on the locations of the source itself or the intermediate nodes. However, for generality, we assume that the entire network has low mobility. Taking into account higher degrees of mobility is part of our ongoing work.

B. Failure Model

We test our routing technique using two different types of failure scenarios, namely, intermittent node failure and the jamming model. The baseline is provided by the case when all nodes in the network function correctly, providing the best possible performance which would degrade with increase of failures.

The first model captures independent node failures. Thus *some* nodes in the network fail, but there is no pattern by which the nodes fail. In reality, isolated failures can take place due to energy dissipation or localized environment effects [4].

The jamming model captures geographically correlated failures, or patterned failures. Such a failure affects all wireless links in a circle of radius R_p. The choice of the circle is somewhat arbitrary, but it attempts to model radio wave propagation. We assume that a *jammer* can operate at any location in the network at a given time. The jammer's power to signal power ratio (JSR) at the receiver determines the degree to which jamming is successful [14]. In our simulation study, we assign actual power levels to jammers and simulate jamming individually for each transmission.

IV. Petal Routing

In this section we present a robust routing scheme, that we call *Petal Routing*. The goal of this approach is to increase reliability while keeping the number of intermediate transmissions to a minimum. Reliability is increased by the use of diffused paths over a geographic region of the network. When the source transmits a packet, it encapsulates the payload with petal headers. We first define a petal packet, which we call a *petalgram*. The headers in a petalgram are as follows.

- Packet ID (*ID*): a number that uniquely identifies a packet
- Source Location (S_{loc}): co-ordinates of the source
- Destination Location (D_{loc}): co-ordinates of the destination
- Transmitter Location (T_{loc}): location co-ordinates of the node that is transmitting (or transmitted) the packet
- Petal Parameter (P): this parameter defines the extent of the diffuse pathset - the actual parameter depends on the specific shape schema being used, as in our example later

In a wireless network, transmissions are inherently broadcast, forming multiple overlapping collision domains. When a node receives a packet, it needs to determine whether or not the packet was intended for it. If not, then it can potentially act as an intermediate node in the transmission, and needs to determine whether it is inside the petal or not, using the location co-ordinates of the source, destination and the petal parameters embedded in the header of the petalgram. The calculation of whether a node is inside a petal has been discussed in section V. To aid in visualizing a petal, consider Fig. 1, where S and D represent the source and destination nodes respectively. If no geographic source-destination path exists within the area of the petal, then it is up to the source to detect failure of transmission using end-to-end acknowledgement. To retransmit a packet, the width of the petal should be increased in order to find such geographic paths. This provides the reactive tuning of our approach.

If an intermediate node is inside the petal, it adds the packet to a waiting buffer B_{wait} after a back-off time, which we discuss in the next section. To avoid flooding loops, all nodes store the IDs of recently broadcasted packets in an array $idList$, allowing them to ensure that any packet is forwarded at most once, even if it is received multiple times. The complete algorithm Schedule_or_drop_packet is shown below.

Algorithm 1 Schedule_or_drop_packet

```
Obtain curent node location $P_{loc}$ and petal headers
if $P_{loc} = D_{loc}$ then
    Destination has received packet. Exit
else
    if $P_{loc}$ is inside petal then
        if $idList[]$ contains $ID$ then
            This packet was already transmitted by this node so
            drop packet. Exit
        else
            Add ID to $idList[]$. Choose back-off time $t_b$. Add
            packet to waiting buffer $B_{wait}$
        end if
    else
        Drop packet
    end if
end if
```

A. Back-off Time

Petal Routing provides a back-off mechanism to reduce medium collisions and the number of transmissions. It should be noted that the number of transmissions is directly related to the probability of collision. The main idea behind introducing back-offs is as follows. Within a petal, all nodes do not need to transmit for the packet to reach the destination. This is more pertinent, if all successors of an intermediate node have already received the packet. When a node receives a packet and finds itself to be inside the petal, a back-off time t_b can be introduced. The node can be made to back-off t_b milliseconds, before it deciding whether to transmit or not. If, within this time, it can hear transmissions from k nodes, then it decides to drop the packet, otherwise it transmits. Note that the value of t_b can vary for individual nodes based on their location with respect to the petal. Knowledge of the node density allows a node to compute the expected value of k, by considering the area represented by the nodes from which transmissions were heard: we describe this in more detail in the next section.

The value of t_b can be selected based on the delay requirements. While the back-off time may reduce the number of transmissions in the network, it may lead to high delays if its value is very large. Thus, there is a trade-off between the delay and the number of transmissions. However, the reliability of transmission is not affected by introducing back-off. Even if the node backs off for a longer period of time, it would eventually transmit the packet if its neighbors did not receive it. We present three methods for selecting t_b.

1) Random Back-off: This is a simple method, in which the value of t_b can be selected as a random number (with some pre-defined upper bound). This would ensure that different nodes back-off for different periods of time. Although there is no pattern in the back-off values of the different nodes, it would still alleviate some medium contention issues.

2) Coordinated Back-off: Using coordinated back-off values based on the location of each node with respect to the petal, provides further heuristic enhancements to reduce the number of individual transmissions. Given a petal, we would like to choose t_b in such a way, that the nodes located towards center of the petal have a higher probability of transmitting the packet first, because the straight line is the most desirable path. Thus, these nodes should have a smaller t_b, while the nodes located near the sides of the petal (or the perimeter of the petal) have a higher value of t_b.

Varying the back-off time based on node locations, we consider that t_b is least along the S-D line (t_{lb}), and it uniformly increases to reach an upper bound (t_{ub}) at the edge of the petal. Thus, when the nodes along the central line transmit first, some of the nodes towards the edges may not have to transmit if they are able to hear transmissions from all the downstream neighbors. This phenomenon is illustrated in Fig. 2(a).

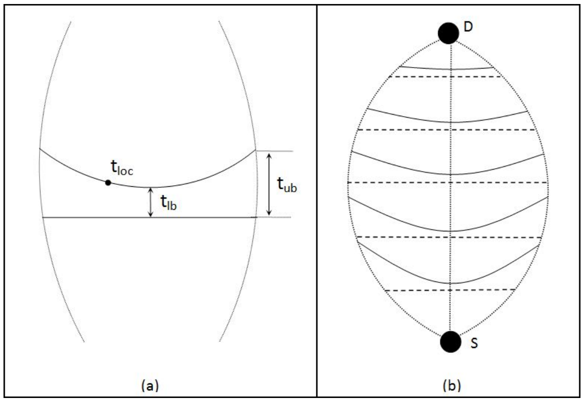

Fig. 2. (a) Curve representing back-off time varying from center of petal to edges (b) Flattening of the curve from source to destination

Further, if a node is made to back-off from its downstream neighbors, then there is a higher chance of the downstream neighbors receiving the packet, without this node's transmission. To realize this phenomenon, we consider that the value of the upper bound of the curve (t_{ub}) decreases from the source to the destination. Any individual node inside the petal would back-off from its more centrally located adjacent nodes, as well as from its downstream neighbors. Thus, the upper bound of t_b is decreased gradually from the source to the destination. In other words, the curve of the back-off values, would become more *flattened* as it approaches the destination. This feature can be visualized in Fig. 2(b).

3) Randomized Coordinated Back-off: This method involves the same steps as in Coordinated Back-off. However, instead of selecting the value on the curve (shown in Fig. 2) at a certain location, a random number between t_{lb} and the value on the curve is selected. This allows for more randomness, rather than choosing a specific value based on the curve. Thus the value of t_b in this case would always be less than or equal to the value from Coordinated Back-off method.

B. Redundancy Tuning

After a back-off time expires, a node has to decide whether it should transmit the packet. The buffer B_{wait} contains a count of the number of nodes from which this node heard the packet as well as the location coordinates of these nodes. If the value of count, is less than k, the expected number of neighboring nodes, the current node would transmit the packet. The value of k is calculated using the node density of the network. We use two standard methods to form a region enclosing the nodes and calculating the expected number of nodes in the region, as follows.

1) Bounding Box: This is a rectangle with minimum area, containing all the nodes that the current node heard from during its back-off period. The area of the rectangle can easily be found. From the nodal density of the network, the expected number of nodes in the bounding box can be found. The node density of a network is defined as the average number of nodes per unit area of the network.

2) Convex Hull: This is a convex polygon tightly containing all the nodes that the current node heard from. The area of the hull is calculated by dividing it into triangles. Once the area is calculated, the expected number of nodes in that region can be calculated assuming uniform nodal density in the network.

Once the region enclosing the neighboring nodes has been computed, the current node checks if it is outside the region. If it is outside, then it is likely that all its *downstream* neighbors have already received the packet. Downstream neighbors are defined as nodes closer to the destination than the current node. In this case, the enclosed region would be in *front* of the current node, towards the destination. However, if the enclosed region is not towards the destination, then the current node would clearly be able to forward the packet to other downstream neighbors. In this case it transmits the packet. To calculate if a certain enclosed region is towards the destination, we calculate a weighted centroid of the actual neighboring node locations and check if the centroid is closer to the destination than the current node. The weighted centroid of the enclosed region is calculated by computing a mean of the neighboring nodes' latitude and longitude coordinates.

If the current node is located inside the enclosed region, then it checks if the number of nodes it heard back from is less than the expected number of nodes in the enclosed area, and if so, it transmits the packet. The expected number of nodes in the enclosed region is calculated using nodal density information. Fig. 3 shows two cases where the current node is inside or outside the enclosed area.

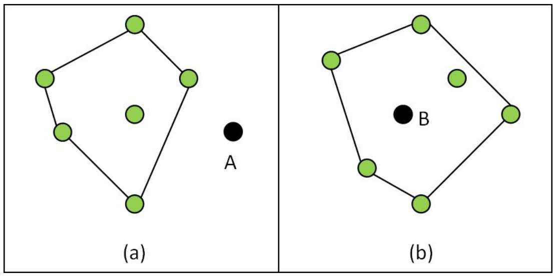

Fig. 3. Determining whether to transmit a packet based on the convex hull

V. Petal Routing Implementation

When a node receives a packet, it needs to determine whether or not it is inside the petal defined by the petalgram headers. Consider the source destination pair in Fig. 4. The source is denoted by the co-ordinates (x_s, y_s) and the destination by (x_d, y_d). Let $P(x_p, y_p)$ be a point. Given the co-ordinates of the source and the destination, as well as the petal parameter, our goal is to determine whether the point P lies inside the petal or not. In our implementation of Petal Routing, we use an ellipse as a specific petal schema; an ellipse is a simple shape that has the desired tapered character, and is easily parameterizable. The petal parameter in our implementation is the minor axis of the ellipse, the major axis connecting the source and destination. The steps to calculate if a given point P is inside the petal are as follows.

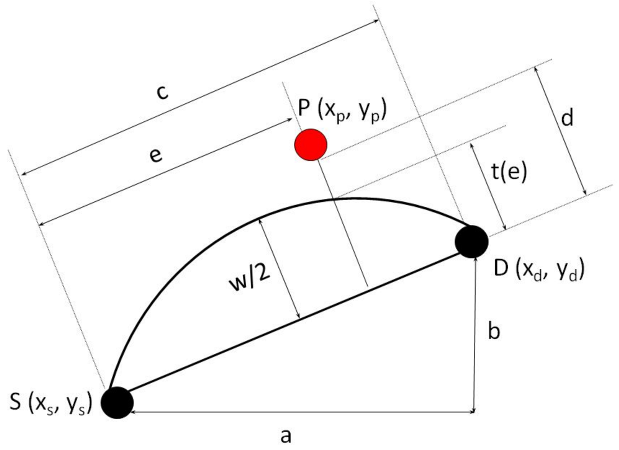
c
P (x_p, y_p)
d
e
t(e)
D (x_d, y_d)
w/2
b
S (x_s, y_s)
a

Fig. 4. Calculating the different petal parameters

The equation of the line though $S(x_s, y_s)$ and $D(x_d, y_d)$ is:

$$(y - y_s) = m * (x - x_s) \tag{1}$$

Distance of point $P(x_p, y_p)$ from the line in equation 1 is:

$$d = \frac{|a(y_s - y_p) - b(x_s - x_p)|}{c} \tag{2}$$

Position along the line in equation 1 where the perpendicular from point $P(x_p, y_p)$ intersects:

$$e = \frac{a(x_p - x_s) + b(y_p - y_s)}{c} \tag{3}$$

where $a = x_d - x_s$, $b = y_d - y_s$, $c = \sqrt{a^2 + b^2}$, $m = b/a$.

Having obtained the point e along the $S-D$ line, we design a threshold function that calculates $t(e)$, the maximum distance from the $S-D$ line to the perimeter of the petal from point e. The function used to calculate $t(e)$ could depend on the shape of the petal used. For example, instead of a petal if we were to use a rectangle shape, then the value of $t(e)$ would be a constant. Using an ellipse, the value of $t(e)$ at point e can be calculated using the formula 4.

$$t(e) = \begin{cases} 0 & \delta < 0 \\ \sqrt{\delta * \beta^2} & \text{otherwise} \end{cases} \tag{4}$$

where $\alpha = c/2$, $\beta = w/2$, $\delta = 1 - \left(\left(e - \frac{c}{2}\right)^2 / \alpha^2\right)$.

VI. Results

We evaluated petal routing using extensive OPNET simulations; due to limited space we present only a small representative subset of results. The nodes were generated randomly using a 2-dimensional Poisson distribution. We compare the three back-off techniques in Fig. 5. The upper bound for back-off is increased from 2 milliseconds to 10 milliseconds in steps of 2. It can be seen that the delay is consistently least for randomized coordinated back-off, as expected.

The objective of back-off is to reduce collisions and therefore repeated transmissions, wasteful of time and energy. In Fig. 6, we see that for all three techniques the total number of transmissions reduces as the back-off time is increased, thereby proving the usefulness of back-off. The three dimensional plot in Fig. 7 shows the interplay between expected reliability, petal width and node failure probability; as the failure probability increases the reliability goes down, but can be improved by widening the petal.

We compare the results of Petal Routing with an existing network coding scheme [2]. The basic approach of the network coding technique is to find k node disjoint paths from source to destination and then send partially overlapping information along the k paths. If at least E_k packets are received by the destination (where $E_k \leq k$), they can be used to reconstruct the original packet. In our implementation of the network coding approach, disjoint paths are computed externally instead of during simulation. This favors the network coding technique, since it eliminates the delay and control traffic overhead in computing node disjoint paths. Fig. 8 shows that with increasing levels of jamming power, the reliability of both approaches reduce. However, the reliability of Petal Routing remains constant for higher levels of jamming power as compared to network coding. Thus, Petal Routing outperforms Network Coding to deliver packets in the presence of jamming attacks.

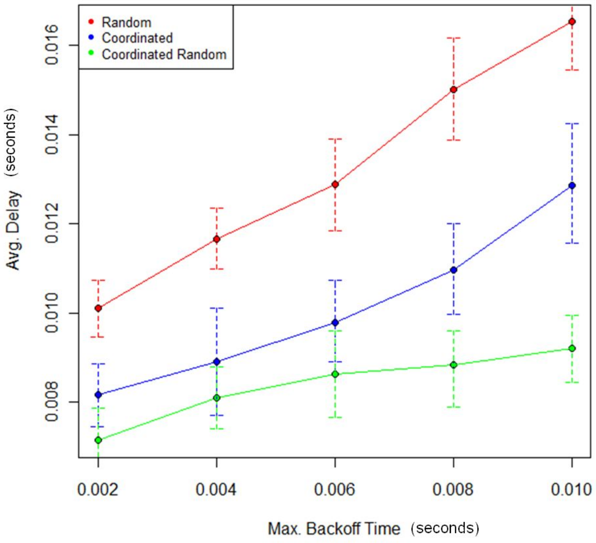

Fig. 5. Delay vs. Back-off time for Petal Routing, 100 node network with no Failures, Petal Width = 0.01, Aggressiveness = 3

VII. Conclusions

We presented a novel routing technique that we call Petal Routing, using multiple paths for increased reliability, but

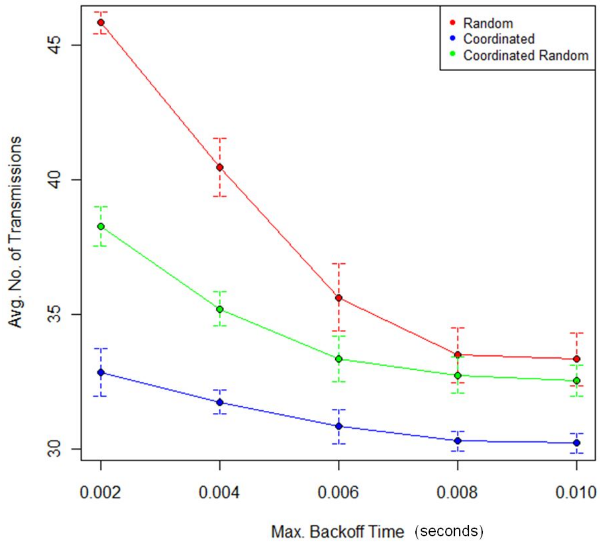

Fig. 6. Number of Transmissions vs. back-off for Petal Routing, 100 node network with no Failures, Petal Width = 0.01, Aggressiveness = 3

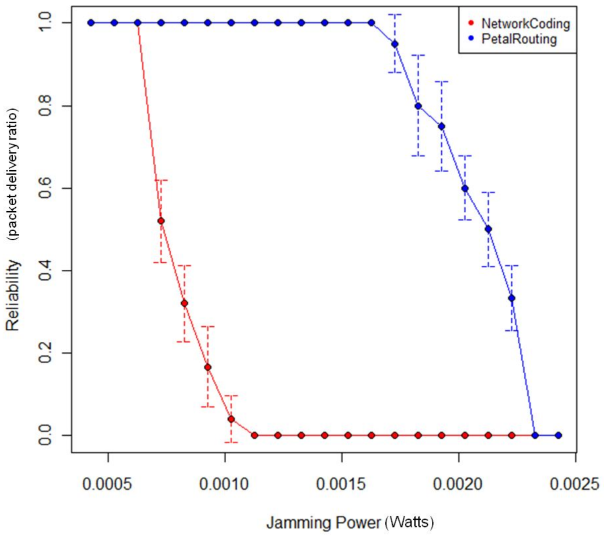

Fig. 8. Reliability vs. Jamming Power (Petal Routing and Network Coding), 100 node network, Petal Width = 0.01, Aggressiveness = 3, Back-off technique = Coordinated, t_{lb} = 0 ms, t_{ub} = 10 ms, Network Coding k = 4, E_k = 2

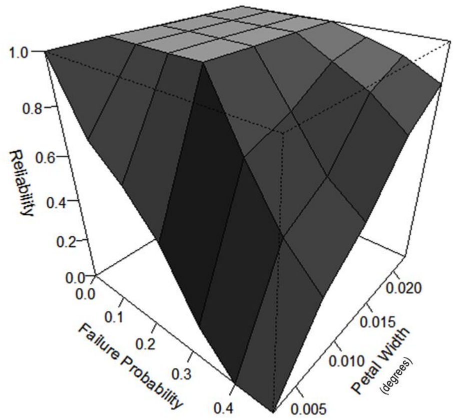

Fig. 7. Reliability vs. Failure probability vs. Petal width for Petal Routing, 150 node network, Back-off technique = Coordinated, t_{lb} = 0 ms, t_{ub} = 5 ms, Aggressiveness = 3

overheard transmissions to reduce wasted transmissions. Using this technique reliability of end-to-end transmissions can be increased in ad hoc networks. We present redundancy tuning techniques along with routing layer back-off to further reduce the number of transmissions and to minimize collisions. Simulation shows that the approach is viable, and behaves as expected. Comparison with an existing network coding technique shows that our approach can result in higher reliability. In ongoing work, we intend to develop an analytical model of the various quantities, as well as addressing node mobility.

REFERENCES

[1] P. Chaporkar and S. Sarkar, “Wireless multicast: theory and approaches,” *Information Theory, IEEE Transactions on*, vol. 51, no. 6, pp. 1954–1972, 2005.

[2] S. Dulman, T. Nieberg, J. Wu, and P. Havinga, “Trade-off between traffic overhead and reliability in multipath routing for wireless sensor networks,” *2003 IEEE Wireless Communications and Networking, 2003. WCNC 2003.*, pp. 1918–1922, 2003.

[3] A. Tsirigos and Z. Haas, “Analysis of multipath routingPart I: The effect on the packet delivery ratio,” *IEEE Transactions on Wireless*, 2004.

[4] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, “Highly-resilient, energy-efficient multipath routing in wireless sensor networks,” *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 4, p. 11, Oct. 2001.

[5] S.-J. Lee and M. Gerla, “Split multipath routing with maximally disjoint paths in ad hoc networks,” *ICC 2001. IEEE International Conference on Communications. Conference Record (Cat. No.01CH37240)*, pp. 3201–3205, 2001.

[6] M. K. Marina and S. R. Das, “Ad hoc on-demand multipath distance vector routing,” *Wireless Communications and Mobile Computing*, vol. 6, no. 7, pp. 969–988, Nov. 2006.

[7] Z. Ye, S. Krishnamurthy, and S. Tripathi, “A framework for reliable routing in mobile ad hoc networks,” in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 1. IEEE, 2003, pp. 270–280.

[8] H. Ammari and S. Das, “A trade-off between energy and delay in data dissemination for wireless sensor networks using transmission range slicing,” *Computer Communications*, vol. 31, no. 9, pp. 1687–1704, 2008.

[9] Y.-B. Ko and N. H. Vaidya, “Location-aided routing (LAR) in mobile ad hoc networks,” *Wireless Networks*, vol. 6, pp. 66–75, 2000.

[10] S. Ruhrup, H. Kalosha, A. Nayak, and I. Stojmenovic, “Message-efficient beaconless georouting with guaranteed delivery in wireless sensor, ad hoc, and actuator networks,” *Networking, IEEE/ACM Transactions on*, vol. 18, no. 1, pp. 95–108, 2010.

[11] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, “Sdar: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks,” in *Local Computer Networks, 2004. 29th Annual IEEE International Conference on*. IEEE, 2004, pp. 618–624.

[12] S. Biswas and R. Morris, “Exor: opportunistic multi-hop routing for wireless networks,” *ACM SIGCOMM Computer Communication Review*, vol. 35, no. 4, pp. 133–144, 2005.

[13] W. Ye, J. Heidemann, and D. Estrin, “An energy-efficient MAC protocol for wireless sensor networks,” in *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 3. IEEE, 2002, pp. 1567–1576.

[14] R. Poisel, *Modern Communications Jamming Principles And Techniques*. Boston, MA, USA: Artech House, 2003.