Reliability Prediction of Diffused Pathset Routing in Wireless Multihop Networks

Trisha Biswas
Department of Computer Science
North Carolina State University
Email: tbiswas@ncsu.edu

Rudra Dutta
Department of Computer Science
North Carolina State University
Email: rdutta@ncsu.edu

***Abstract*—Wireless multihop networks such as ad hoc and mesh networks are susceptible to both random uncertainty of radio links and malicious jamming. Traditional unipath routing techniques reduce the overall packet delivery ratio in presence of network failures. Being able to predict the reliability of a transmission a priori can be useful in designing reliable networks. We consider a network of nodes addressed by their locations carrying out redundancy-based routing, and propose an analytical model that can predict the reliability of a transmission given certain parameters such as network node density and region of network involved in the transmission. For this study we consider a geo-diffuse multipath routing technique called Petal routing, which takes advantage of the broadcast nature of wireless networks to reduce the number of transmissions for multiple paths. We investigate the accuracy of the analytical model by comparing metrics such as reliability obtained from the model and from OPNET simulations.**

***Index Terms*—Wireless multihop networks, redundancy, diffuse pathsets, failures, analytical model, minimal cutset.**

I. Introduction

Multihop wireless networks use two or more wireless hops to convey information from a source to a destination. Challenges of multihop networks include the inherent uncertainty and vulnerability of the wireless medium that gives rise to difficulty in guarding against failures of path transmissions. Failures due to the medium are usually observed as intermittent or random link failures. Geographically correlated link failures could be actively caused by malicious network elements such as jammers. Reliability of transmissions in wireless networks heavily depend on the design of routing protocols. Redundancy is a common technique used for achieving reliability in networks prone to failures. Redundancy is often realized by sending the data over multiple paths from the source to the destination, if the network is well connected. Many redundant routing techniques exist in the literature such as [1]. Since redundancy increases the number of intermediate transmissions, there exists a tradeoff between reliability and traffic overhead. The goal of our research in this paper is to predict the reliability of an end-to-end transmission given other network parameters.

For our study, we use a geo-diffuse routing technique called Petal routing [2], which utilizes diffuse pathsets between the source and the destination. The number of diffuse pathsets can be varied based on reliability requirements of the network. The 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. Based on this redundant routing technique, we present an analytical model, that can predict the reliability of a given transmission. We define reliability to be a mission-specific metric: the probability that the message will reach its destination. We focus on establishing an analytical relationship between the routing parameters and the level of reliability achievable. A brief description of the mechanism and parameters for the approach is provided, further details can be found in [2].

We also present an extended form of Petal routing that can be used to reduce the number of intermediate transmissions. The basis of this redundancy tuning procedure can be found in [2] by the use of a backoff timer. We present a novel technique using "cancellation score", to reduce transmissions after the backoff timer at a node expires. Finally, we present an analytical model to predict reliability of a transmission for Petal routing with redundancy tuning. This technique builds on the analytical model for basic Petal routing.

II. Related Work

Reliability of transmissions can be increased with multipath routing in presence of network failures [3]. Jammers or malicious nodes pose serious threats to the distributed environment of wireless networks and can successfully disrupt a network [4]. Reliability of wireless networks has been studied previously [5], [6]. Many of the techniques in wired networks use enumeration of cutsets to analyze failures in the network. In graph theory, a cut is a partition of the vertices of a graph into two disjoint subsets. The cutset of the cut is the set of edges whose end points are in different subsets of the partition. Cutsets are used in reliability analysis because any cut that partitions the source and the destination into two subsets, would cause a transmission failure. Our method of predicting reliability is also based on computation of minimal cutsets of the network. We tailor the approach to address specific characteristics of the diffused pathset algorithm studied.

III. Geo-diffuse Pathsets: Petal Routing

In this section, we provide a brief overview of the routing technique described in [2]. 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. All nodes within the region defined as the petal aid in the transmission by broadcasting the packet. Intermediate nodes can compute whether they are located *inside* the petal, using their node location, and other information embedded in the packet header, namely, the source location, destination location and a petal parameter. This parameter quantifies the region of constrained flooding and depends on the specific shape schema being used. Intuitively, we call this parameter to be the 'width' of the petal. An example of a schema could be to use an ellipse to represent the petal, and the parameter in this case could be the minor axis of the ellipse, while the major axis would connect the source and destination. Further details on how an ellipse can be used to represent the petal can be found in [2]. For a given end-to-end transmission, the width of the petal is constant; if the transmission fails due to intermediate link failures, re-transmission is carried out with an increased petal width.

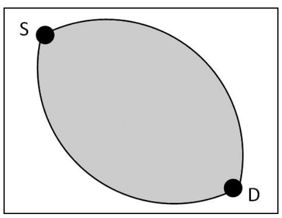

Fig. 1. Diffused overlapping pathsets

As in other geographic routing techniques [7], Petal routing uses node locations to uniquely identify nodes. Messages are routed to the location of the destination rather than a network address. It is assumed that a node always knows its current location. Additionally, the source knows the location of the destination. Nodes do not need to maintain any routes to other nodes or know who their neighbors are. When the source transmits a packet, it encapsulates the payload with petal headers such as packet ID, source location, destination location, and width of the petal. When a node receives a packet, it needs to determine whether or not the packet was intended for it. If not, then it is an intermediate node in the transmission, and it now needs to determine whether it is inside the petal or not. The basic algorithm followed by a node upon receiving a packet is given in Algorithm 1. To avoid flooding loops, all nodes store the IDs of recently broadcasted packets in an array that we call $idList[]$, subject to size constraints.

Algorithm 1 Algorithm for Basic Petal Routing

```
Obtain curent node location co-ordinates: P_loc
Get petal headers: ID , S_loc, D_loc, T_loc, W
if P_loc = D_loc then
  Destination has received packet
  Exit
else
  Determine if node P is inside the petal
  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
      Transmit the packet
      Add ID to idList[ ]
    end if
  else
    Drop packet
  end if
end if
```

Note that any cutset of the petal would cause a transmission failure. To calculate all possible ways in which a transmission would fail, one would have to compute all cutsets of a given network. We present a technique that starts with all possible *minimal* cutsets of the petal.

IV. Analytical Model for basic Petal Routing

The analytical model for Petal routing takes a set of input parameters and calculates the expected reliability of the transmission. Input parameters include network node density, range of each node, overall link failure probability, width of the petal and distance between the source and destination. The basic idea behind the analytical model is as follows. An end-to-end transmission can fail only if a combination of paths fails such that it converts the petal into a disconnected graph.

A. Terminology

Graph $G = (V, E)$ consists of a set V of vertices and a set E of edges, and a relation that associates each edge with a pair of vertices. Edge $e = (u, v) \in E$ and is said to be incident with vertices u and v, where u and v are the end points of e. In an undirected graph G, two vertices u and v are said to be connected if G contains a path from u to v. If the two vertices are additionally connected by a path of length 1, they are called adjacent. The set of vertices adjacent to v is written as $A(v)$, and the degree of v is the number of vertices adjacent to v and is denoted as $|A(v)|$

A graph is said to be connected if every pair of vertices in the graph is connected. We only consider connected graphs in this study. A graph H is a subgraph of G if $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$. H is an induced subgraph of G if every pair of vertices in $V(H)$ that are adjacent in G are also adjacent in H. $G[S]$ denotes the subgraph of G induced by the set of vertices S. A connected component of G is a maximal connected subgraph of G.

Definition 1: A cut is a partition $\langle X, X' \rangle$ of graph $G = (V, E)$ into two proper disjoint subsets of V. The complement of $X \subseteq V$ is denoted as $X' = V - X$.

A network is a directed graph with one or more vertices labeled as the producing source, and one or more labeled as the consuming sink. For our study, we consider networks with a single source and a single sink.

Definition 2: In a network, a source/sink cut $\langle S, T\rangle$ is a partition with $s \in S$ and $t \in T$.

Definition 3: The cutset $C = \{(u, v) \in E | u \in X, v \in X'\}$ of the cut $\langle X, X'\rangle$ is the set of edges whose end points are in different subsets of the partition. The size of a cut is the number of edges in the cutset.

Definition 4: A cutset is said to be a minimal cutset if, when any edge $e \in C$ is removed from it, the remaining set $C' = C - \{e\}$ is no longer a cutset of G.

B. Analytical Model

For a graph, the set of minimal cutsets provides the smallest number of ways in which a transmission can fail. We extend the set of minimal cutsets to account for all possible failure scenarios using other network parameters such as the overall link failure probability to model Petal routing closely. We consider each minimal cutset to be a family of failures and then try to enumerate the number of actual failures scenarios each such set represents. We first compute all minimal cutsets for a given network, defined by all the nodes inside the petal. We use the technique outlined in [8] to enumerate all minimal cutsets in linear time per cutset. Let all cutsets of a petal be denoted by $C = \{c_1, c_2, ..., c_k\}$, where there are k minimal cutsets. We consider the petal to consist of l links and p_l to be the overall link failure probability of the network. Given p_l, $max(c)$ is the maximum number of links that can fail in the network. For a given cutset, $E(e_{fail})$ is the expected number of links that can fail. The remaining number of links that are expected to fail leading up to the cut is denoted by $E(e'_{fail})$. The number of different ways in which the remaining links ($E(e'_{fail})$) can fail out of the links located *before* the cutset is denoted by $E(c_{fail})$. We use the term "cousins" to loosely describe all failure scenarios that include the cutset under consideration. For reliability analysis, we do not need the exact combination of links that fail for each scenario, and thereby, we reduce a combinatorial problem to a counting problem.

For each failure scenario, the failure probability can be calculated as,

$$p_{fail} = (p_l)^f * (1 - p_l)^s \quad (1)$$

where p_l is the link failure probability, f is the number of failed links and s is the number of successful links. Formula 1 can be extended for all cousins of this cutset using the formula,

$$p_{c_i} = E(c_{fail}) * (p_l)^f * (1 - p_l)^s \quad (2)$$

where $E(c_{fail})$ represents the number of ways in which $E(e'_{fail})$ links can fail out of all the links before the cutset. Note that in computing p_{c_i} as shown above, we assume that exactly $E(e_{fail})$ links fail. Since this is an expectation, in reality it may not be the case although it is highly probable. $E(e_{fail}) \pm l'$ links can fail, with diminishing probability as l' increases. In Section VII, we first present results assuming that exactly $E(c_{fail})$ links fall, and then explore concept of greater-than or less-than $E(e_{fail})$ links failing.
Since each minimal cut's contribution to the overall failure probability is independent, the value of p_{c_i} for each minimal cutset is summed up, and finally, the reliability of the transmission can be calculated as,

$$Reliability = 1 - \sum_{i=1}^{k} p_{c_i} \quad (3)$$

The complete set of steps to calculate the reliability of a given transmission can be found in Algorithm 2.

Algorithm 2 Calculate reliability for basic Petal routing

Inputs: Graph $G(v, l)$ (consisting of all nodes inside the petal), link failure probability (p_l), source location (S), destination location (D)

$max(c) = floor(p_l * l)$
Compute all minimal cutsets, $C = \{c_1, c_2, ..., c_k\}$, for k cutsets

for $i = 1 \to k$ **do**
  if $|c_i| \le max(c)$ **then**
    e = number of edges before the cut
    $E(e_{fail}) = floor(p_l*(e+|c_i|))$ //Expected failed links
    if $|c_i| \le E(e_{fail})$ **then**
      $E(e'_{fail}) = E(e_{fail}) - |c_i|$ // Remaining links to fail
      $p_{c_i} = {}^{e}\mathcal{C}_{E(e'_{fail})} * (p_l)^{E(e_{fail})} * (1 - p_l)^{(e+|c_i|-E(e_{fail}))}$
    end if
  end if
end for
$p_c = \sum_{i=1}^{k} p_{c_i}$
$Reliability = 1 - p_c$

V. Petal Routing with Redundancy Tuning

Petal routing provides a mechanism to reduce the number of intermediate transmissions for nodes located inside the petal. The basis of this idea is presented in [2]. It stems from the fact that not all nodes inside the petal need to retransmit the packet. Instead, if some nodes cancel transmission without affecting the overall reliability, the number of retransmissions can be reduced. The challenge lies in identifying such nodes inside the petal. We provide a brief discussion on redundancy tuning, and then present a novel mechanism to reduce the number of intermediate transmissions. This can be considered to be an extension of the mechanism presented in [2].

A. Backoff

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 backoff time t_b can be introduced. The node can be made to backoff 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: this has been described in Section V-B.

The value of t_b can be selected based on the delay requirements. While the backoff 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 backoff. This is because of the fact that 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. This would cause a greater delay, but would not affect the reliability of transmission. With the introduction of backoff time, the steps for Petal routing is presented in Algorithm 3.

Algorithm 3 Algorithm for Petal Routing with Backoff

```
Obtain curent node location co-ordinates: P_loc
Get petal headers: ID , S_loc, D_loc, W, S_t, L_hop
if P_loc = D_loc then
  Destination has received packet
  Exit
else
  Determine if node P is inside the petal
  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 backoff time t_b
      Add packet to waiting buffer B_wait
    end if
  else
    Drop packet
  end if
end if
```

B. Redundancy Tuning

After the backoff timer expires, a node has to decide whether it would cancel the transmission or not. In this section, we present a novel mechanism for intermediate nodes to cancel pending transmissions. When the timer expires, the node knows the number of neighboring nodes from which it heard the packet as well as the location coordinates of the neighbors. Using this information, the node computes a value, that we call the 'cancellation score' or S_c. Intuitively, cancellation score is a number that indicates how aggressively a node should cancel its transmission. A high cancellation score indicates that the probability of transmission should be very low. We present a method to compute the cancellation score and map the value to link transmission probability ranging from 0 to 1.

Figure 2a illustrates a sample scenario after a backoff timer expires. Node P is the current node, while C is the location of the weighted centroid of all the neighboring nodes P heard from while it was backing off. $|PP'|$ is the perpendicular distance of P from the SD line, while CC' is the perpendicular distance of C from the SD line. We compute the cancellation score using Formula 4.

$$S_c = k * \left(\frac{|PD|}{|SD|}\right) * |PP'| * |CC'| * |PC| * neighborCount \quad (4)$$

where k is a constant, $neighborCount$ is the number of nodes P heard from and the remaining parameters are consistent with Figure 2a.

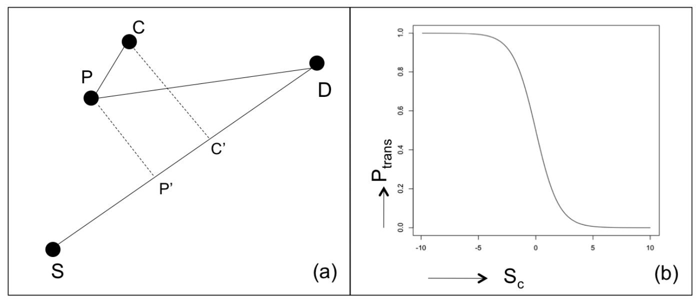

Fig. 2. (a) Calculation of cancellation score S_c; (b) Inverse sigmoid curve

The justification for using Formula 4 is as follows. The geographic source destination line is closest to the shortest path between S and D. Transmissions close to the source destination line should therefore be canceled rarely. Also, if $neighborCount$ is very low, the cancellation score would also be low, and the node would be more likely to transmit regardless of its deviation from the SD line. Transmissions closer to the destination should be canceled less aggressively so that the overall transmission has a higher likelihood of succeeding. Lastly, the term $|PC|$ indicates how far the centroid is from node P. It also captures whether C is closer to the destination than P. If C is further away from the destination than P we assign this value to be negative.

In order to map the cancellation scores to probability values, we use an inverse sigmoid curve shown in Figure 2b with the pivot at $x = 0$. According to the inverse sigmoid curve, the higher the cancellation score is, the lower the probability of transmission is and vice versa. For negative values, P_{trans} ranges from 0.5 to 1, i.e., if the centroid is behind P the node is highly likely to transmit the packet because it can reach more nodes in front of it. The formula for the sigmoid curve is as follows:

$$P_{trans} = \left(\frac{1}{1 + e^x}\right) \quad (5)$$

where x is the cancellation score, or the x-axis of the curve from Figure 2b.

VI. Analytical Model for Petal Routing with Redundancy Tuning

For fine grained results from the analytical model, we propose to vary the failure probability of a link based on a node's location with respect to the petal. The degree of variation can be directly based on the node cancellation behavior observed in Section V-B. Based on the maximum backoff value, we can obtain the average $neighborCount$ and average distance $|PC|$ for a network with certain node density, from simulations. These values are provided as input to the analytical model. We use the cancellation score formula from Section V-B, to directly vary the failure probability of a link. We compute the cancellation score of the starting and ending nodes (S_{c_1} and S_{c_2}) of each link using Formulae 4. We then compute the mean link transmission probability using the sigmoid function from Formula 5. To obtain the cancellation probability for the link p_{e_j} we subtract the link transmission probability from 1. p_{e_j} is the failure probability for link e_j in addition to the overall link failure probability p_l. Note that p_{e_j} would be minimum along the backbone of the petal and maximum along the perimeter.

We compute p_{e_j} for each link of a given minimal cut. The probability of the links of the minimal cut failing p_e, is then given by:

$$p_e = \prod_{j=1}^{|c_i|} \frac{(p_{e_j} + p_l)}{2} \quad (6)$$

In the above formula, the probability of a link in the minimal cut is weighted based on the cancellation score obtained from its location inside the petal. To calculate the failure probability of a cut p_{c_i}, we use the following formula:

$$p_{c_i} = {}^{e}\mathcal{C}_{E(e'_{fail})} * (p_l)^{(E(e_{fail})-|c_i|)} * (1-p_l)^{(e+|c_i|-E(e_{fail}))} * (p_e) \quad (7)$$

The complete set of steps to calculate the reliability with backoff can be found in Algorithm 4.

Algorithm 4 Calculate reliability for Petal routing with Backoff

Inputs: Graph $G(v, l)$ (consisting of all nodes inside the petal), link failure probability (p_l), source location (S), destination location (D), average distance $|PC|$, average $neighborCount$

$max(c) = floor(p_l * l)$
Compute all minimal cutsets, $C = \{c_1, c_2, ..., c_k\}$, for k cutsets

for $i = 1 \to k$ **do**
  if $|c_i| \leq max(c)$ **then**
    e = number of edges before the cut
    $E(e_{fail}) = floor(p_l * (e + |c_i|))$
    if $|c_i| \leq E(e_{fail})$ **then**
      for each edge j in cut c_i **do**
        P_1 is the starting node for the edge j
        Compute point C_1, $|PC|$ distance away from P_1, parallel to SD line
        Compute point P_1', perpendicular projection of P_1 on SD line
        Compute point C_1', perpendicular projection of C_1 on SD line
        $S_{c_j} = k * \left(\frac{|P_1 D|}{|SD|}\right) * |P_1 P_1'| * |C_1 C_1'| * |P_1 C_1| * neighborCount$
        $p_{e_j} = 1 - \left(\frac{1}{1+e^{S_{c_j}}}\right)$
      end for
      $p_e = \prod_{j=1}^{|c_i|} \frac{(p_{e_j}+p_l)}{2}$ // Failure probability of links of cut c_i
      $E(e'_{fail}) = E(e_{fail}) - |c_i|$
      $p_{c_i} = {}^{e}\mathcal{C}_{E(e'_{fail})} * (p_l)^{(E(e_{fail})-|c_i|)} * (1 - p_l)^{(e+|c_i|-E(e_{fail}))} * (p_e)$
    end if
  end if
end for
$p_c = \sum_{i=1}^{k} p_{c_i}$
$Reliability = 1 - p_c$

VII. Results

We implemented Petal routing over the IP layer using the *manet_station_adv* model in OPNET.

A. Results for basic Petal Routing

Figure 3 shows a plot of reliability versus increasing petal width for OPNET simulations and the analytical model for a 200 node perturbed grid topology using Algorithm 2. It can be seen that the analytical model provides an upper bound on the reliability value.

Figure 4 shows a comparison of different 150 node clustered topologies generated using a uniform random number generator. We show three variations of topologies in the analytical model, (1) by providing the exact topology, (2) by using generated topologies and (3) using sample topologies generated by OPNET. The reliability values obtained by generated topologies were closer to simulations than sample topologies from OPNET. This may be because the sample set from OPNET was not as representative.

B. Results for Petal Routing with Redundancy Tuning

Figure 5 shows a plot of reliability versus petal width for a 200 node perturbed grid topology for petal routing with backoff, where the topology was provided to the analytical model (using Algorithm 4).

Figure 6 shows a similar plot for a 150 node clustered topology where the topology was not provided to the analytical model. With clustered topologies the results from the analytical model deviate from simulations, and this is an expected artifact of the clusteredness of the topology.

VIII. Conclusions

In this study we present an analytical model to predict the reliability of a given transmission using a redundant routing

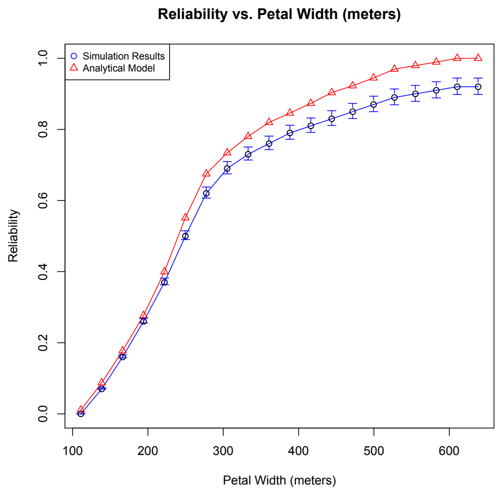

Fig. 3. Reliability vs. Petal Width for Simulations and Analytical Model. Topology provided to analytical model

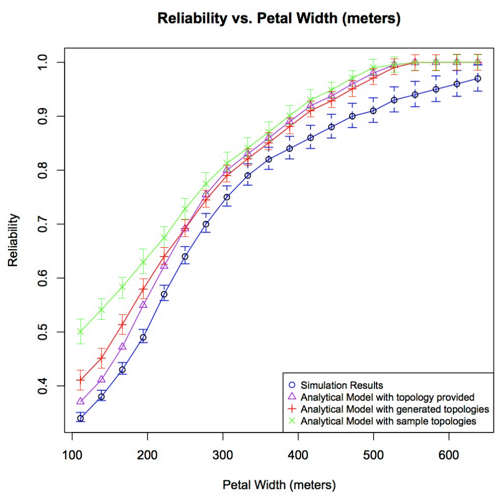

Fig. 4. Reliability vs. Petal Width for Simulations and Analytical Model with different topology techniques

technique called Petal routing. Using this predictive procedure, one can get the probability of packet transmission succeeding. We also present some extensions to Petal routing, in order to cancel intermediate transmissions after the backoff timer expires. The comparative results for both analytical models demonstrate that they can successfully predict the reliability of a given end-to-end transmission.

REFERENCES

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

[2] T. Biswas and R. Dutta, "Spatially diffuse pathsets for robust routing in ad hoc networks," in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*. IEEE, 2011, pp. 1–6.

[3] 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.

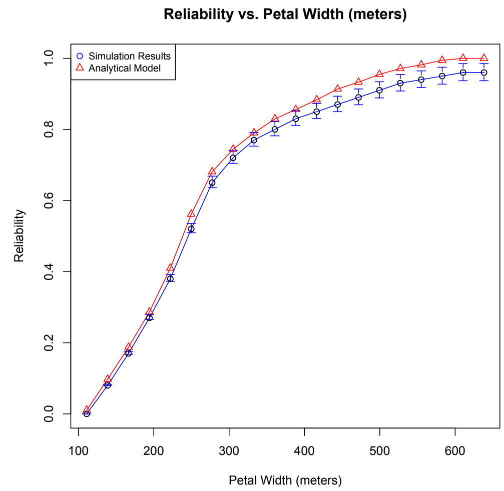

Fig. 5. Reliability vs. Petal Width, 200 node perturbed grid topology provided to analytical model, using Petal routing with backoff

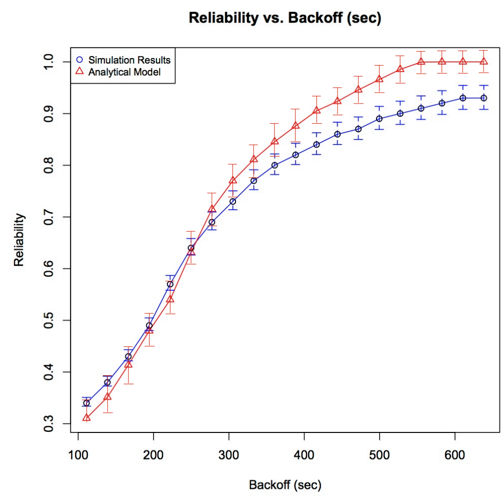

Fig. 6. Reliability vs. Petal Width, 150 node clustered topology, not provided to analytical model, using Petal routing with backoff

[4] U. Patel, T. Biswas, and R. Dutta, "A routing approach to jamming mitigation in wireless multihop networks," in *Local & Metropolitan Area Networks (LANMAN), 2011 18th IEEE Workshop on*. IEEE, 2011, pp. 1–6.

[5] H. AboElFotoh, S. Iyengar, and K. Chakrabarty, "Computing reliability and message delay for cooperative wireless distributed sensor networks subject to random failures," *Reliability, IEEE Transactions on*, vol. 54, no. 1, pp. 145–155, 2005.

[6] M. Ghaderi, D. Towsley, and J. Kurose, "Reliability gain of network coding in lossy wireless networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008, pp. 2171–2179.

[7] 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.

[8] A. Sharafat and O. Ma rouzi, "Recursive contraction algorithm: a novel and efficient graph traversal method for scanning all minimal cut sets," *Iranian Journal of Science and Technology*, vol. 30, no. B6, p. 749, 2006.