A Routing Approach to Jamming Mitigation in Wireless Multihop Networks

Umang Patel
QualComm Inc.
umangspatel@gmail.com

Trisha Biswas
North Carolina State University
tbiswas@ncsu.edu

Rudra Dutta
North Carolina State University
dutta@csc.ncsu.edu

***Abstract*—Wireless networks are susceptible to localized disruptions, due to the shared nature of the medium. Radio jamming, the most common type of localized disruption causes wireless link failures. Jamming mitigation has been traditionally addressed in the physical and MAC layers. Such approaches come with added complexity and often require specialized hardware. We investigate whether a generally applicable routing layer approach, based on multipath routing coupled with power control, can mitigate the effects of jamming. We propose (1) proactive protection and (2) reactive protection techniques for jamming mitigation in wireless multihop networks with fixed nodes. For reactive protection, we propose a distributed geographic routing algorithm that finds alternative route to the destination, starting from the first node with failed link on the original path. We evaluate the performance of this algorithm using OPNET simulations.**

***Index Terms*—Localized disruption, jamming mitigation, ad hoc network, proactive protection, reactive protection, geographic routing.**

I. Introduction

Wireless multihop networks are being considered a viable alternative for metropolitan or campus area networks, especially retrofit [1], [2]. Since critical services may flow over such networks, prevention of localized disruption is of realistic importance in such networks. Wireless communication is susceptible to localized disruptions due to the shared nature of wireless medium. Such disturbances disrupt network traffic and are often viewed as a DoS (Denial of Service) attack localized in space and time. In this paper, we focus on the most common type of localized disruption - jamming. Radio jamming has immediate and direct impact on the physical and MAC (Medium Access and Control) layers functionalities. Packet delivery ratio at the MAC layer drops significantly in the presence of powerful jamming. Research on mitigation of the effects of jamming is typically focused on the MAC [3] and physical layers enhancements. However, physical and MAC layer enhancements cannot defend against jamming beyond a certain limit. IEEE 802.11b based devices can be jammed by a relatively low power jammer, even though IEEE 802.11b has DSSS physical layer. It is becoming relatively easy to build a sophisticated radio jammer due to the availability of configurable radio platforms such as GNU Radio, Cognitive Radio etc. An approach to jamming mitigation by using network layer (forwarding/routing) strategies designed specifically with this in mind can be expected to provide complementary strengths to lower layer approaches.

Network layer approaches have so far not received much attention in jamming mitigation literature, though the effects of jamming on the network layer have been studied. Previously, [4], [5] have considered the impact of jamming on network connectivity and throughput. Simulations results in [5] show that a jammer using higher power than the target network nodes causes substantial number of links failures and the network loses its connectivity. Simulations results in [4] show that a large number of distributed, low power jammers in the target network area causes substantial reduction in the network throughput and increases end-to-end delay in the network. Distributed low power jammers are energy efficient, hard to detect and can survive for a long time. These studies suggest that it is important to consider jamming effects not only at physical and MAC layers, but also at network layer. Moreover, effective jamming defense techniques at MAC and physical layers typically require hardware enhancements [6] and hence they cannot be deployed easily to existing networks. Based on the above findings, we focus on a generally applicable routing approach for mitigating jamming effects in wireless multihop networks with fixed nodes.

We build our approach by utilizing geographic routing techniques. Geographic routing has been studied extensively in the past [7]–[9]. Sending redundant information over multiple paths is a common method to reduce end-to-end transmission failures [10]. This method works well for intermittent, uncorrelated link failures. However, link failures caused due to a jammer are geographically correlated. Our approach is designed specifically to provide protection in presence of such correlated link failures by finding multiple geo-diverse paths using geographic routing. We propose two techniques, namely, proactive protection and reactive protection. The goal of proactive protection is to prevent disruptions in the network traffic caused by jamming. The goal of reactive protection is to restore network traffic which has been disrupted by jamming. The proactive protection technique is applicable when jamming conditions in the network (e.g. jammer's maximum power, number of jammers etc.) are known to network nodes. Reactive protection is applicable when jamming conditions in the network are unknown to network nodes. In the latter approach, an alternate route to the destination node is discovered on-the-fly, when any link on the path from a source to a destination fails due to jamming. Both the reactive and proactive techniques produce geo-diverse multipaths that avoid the jammed region in the network.

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.

II. Related Work

A jammer's presence cannot be concluded definitively by using simple statistics (e.g. energy on channel, carrier sensing time, packet delivery ratio) [11]. MAC parameters (e.g. contention window size) can be tweaked within the standard imposed limit [12] such that a compromised network node can consume much of the available bandwidth and starve other nodes without getting detected. The boundary of nodes in the jamming area can be computed using the distributed area mapping protocol in [13]. Jamming area mapped by the algorithm is useful for other network services (e.g. routing) to avoid the jammed region. MAC layer protocols [3], provide effective and energy efficient algorithms for intelligent jamming. Channel surfing and spatial retreat are other techniques that can be used for jamming defense [14].

III. Jamming Effects Modeling

In a typical jamming scenario, network nodes in the jammed region constantly find the medium busy due to higher energy (noise) on the medium. Due to the lack of an opportunity to transmit, they lose connectivity to the rest of the network. In this section, we present some techniques to model jamming effects for networks that use adaptive energy threshold for CCA. We choose the R_n propagation model for modeling because it is widely applicable to both indoor and outdoor environments by selecting an appropriate path loss exponent.

A. R^n Propagation Model

Theoretical and empirical results show that the average received signal power decreases exponentially with an increase in the distance between the transmitter and receiver [15]. As per the R^n propagation model, path loss at a receiver with the distance d from a transmitter is given by equation 1.

$$PL(dB) = PL(d_0) + 10\log_{10}\left(\frac{d}{d_0}\right)^n \tag{1}$$

where d_0 is a reference point near the transmitter with known path loss $PL(d_0)$, n is the path loss exponent which indicates the rate at which path loss increases with the distance.

Absolute received power based on the R^n propagation model is given by the equation 2 [16].

$$P_R = \frac{P_T G_T G_R}{10^{(PL(d_0)+10\log_{10}(d/d_0)^n)/10}} \tag{2}$$

where P_R is received power, P_T is transmit power, G_T is transmit antenna gain, G_R is receive antenna gain and other terms have the same meaning as in the path loss equation 1.

B. Jamming-to-Signal Ratio (JSR)

The jamming power to signal power ratio (JSR) at the receiver determines the degree to which the jamming is successful. The jammer's goal is to raise JSR to a level where BER (Bit Error Rate) in the network traffic exceeds a certain threshold (e.g. 10^{-2}). No coding scheme can recover corrupted bits at high BER and hence the link fails for the duration of jamming. [16] derives JSR formula based on R^n propagation model as shown in the equation 3.

$$JSR = \frac{Jamming\ power\ received}{Signal\ power\ received}$$

$$= \frac{\frac{P_J G_{JR} G_{RJ}}{10^{(PL(D_0)+10\log_{10}(D_{JR}/D_0)^n)/10}}}{\frac{P_T G_{TR} G_{RT}}{10^{(PL(D_0)+10\log_{10}(D_{TR}/D_0)^n)/10}}}$$

$$= \frac{P_J}{P_T}\left(\frac{D_{TR}}{D_{JR}}\right)^n \tag{3}$$

where P_J is jamming signal's transmit power, P_T is signal's transmit power, G_{JR} and G_{RJ} are transmit and receive antenna gains for the jamming signal, G_{TR} and G_{RT} are transmit and receive antenna gains for the transmitted signal, D_{TR} is the distance between transmitter and receiver, D_{JR} is the distance between jammer and receiver, D_0 is a reference point where path loss $PL(D_0)$ is computed and n is the path loss exponent. We assume that ground characteristics between a transmitter and a receiver and between a jammer and a receiver are the same and hence $PL(D_0)$ is same for both the transmitted signals and the jamming signals. We also assume that antenna gains are same for both the transmitted signals and the jamming signals.

C. Jamming Vulnerability of a Link

Jamming vulnerability of a link is a region around the receiver in which the jammer's presence causes link(s) to fail. Jamming vulnerable region is considered circular under simple constant range model and the region is termed as a **jamming circle**. Jamming circle radius formula 4 is derived from the JSR formula 3 by rearranging the terms.

$$D_{JR} = D_{TR}\left(\frac{P_J}{P_T \times JSR}\right)^{1/n} \tag{4}$$

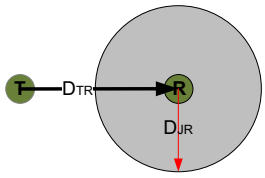

Fig. 1. Jamming Vulnerability of a Link

D. Jamming Vulnerability of a Path

If the jammer's power and minimum JSR to break a link are given, then jamming circle radius for each link on a path can be found using the equation 4. Jamming vulnerability of a path is the total region occupied by these jamming circles. Figure 2 shows an example of jamming vulnerability of a path.

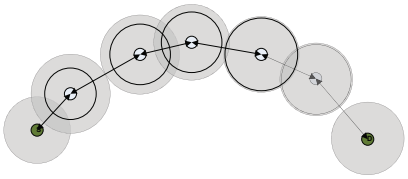

Fig. 2. Jamming Vulnerability of a Path

IV. Proactive Protection against Jamming

The proactive approach to prevent jamming involves routing data redundantly along node disjoint paths. Power control on the links of the node disjoint paths help defend against simultaneous jamming of such paths. We first present a technique to select node disjoint paths and then discuss the steps involved in proactive protection.

A. Multipath Routing and Power Control Approach

Assume that jamming conditions in the network (number of jammers, jammer's maximum power and jamming strategy - BBN, PBN etc.) are known to the network nodes. Distributed jamming detection and localization techniques [11] can provide this information to the network nodes. Using this information, the jamming vulnerable region for a traffic flow which uses a single path, can be computed as described in section III-D. We propose a multipath routing and power control approach for reducing jamming vulnerability of the traffic flow. In this approach, a traffic flow is routed redundantly on node disjoint paths and power control is performed on the links of the node disjoint paths. Redundant routing on the node disjoint paths ensures that any one path's failure due to jamming doesn't disrupt the traffic flow. Power control on the links of the node disjoint paths is required to defend against simultaneous jamming of the paths by a jammer. Power control is performed such that the following two conditions are satisfied:

1. Jamming vulnerable regions around the source and destination of the node disjoint paths are minimum possible.
2. Jamming circles around the intermediate nodes on one path do not overlap with any jamming circles on the other paths.

Figure 3 shows an example of the two node disjoint paths satisfying conditions 1 and 2.

B. Algorithm for Preplanned Protection

Based on the multipath routing and power control approach, we describe the steps involved in providing proactive protection against a single jammer. For a given source and destination in the network, power is assigned to links of distinct path pairs. Power assignment on the links is carried out such that conditions 1 and 2 from the section IV-A are satisfied. For a given path pair (A, B), the jamming circle radius for intermediate nodes on the paths A and B are found, such that condition 2 from the section IV-A is satisfied. If there is no power assignment that satisfies condition 2 from section IV-A, then path pair (A, B) is ignored. The end nodes for a path-pair (A, B) are assigned the maximum allowed power, if condition 1 is already satisfied. This ensures that jamming circles around the end nodes are minimum possible and condition 2 is satisfied. These steps are carried out for all possible path pairs and the pair for which the total assigned power is minimum is chosen. The worst case running time for this algorithm is is $O(n^2)$.

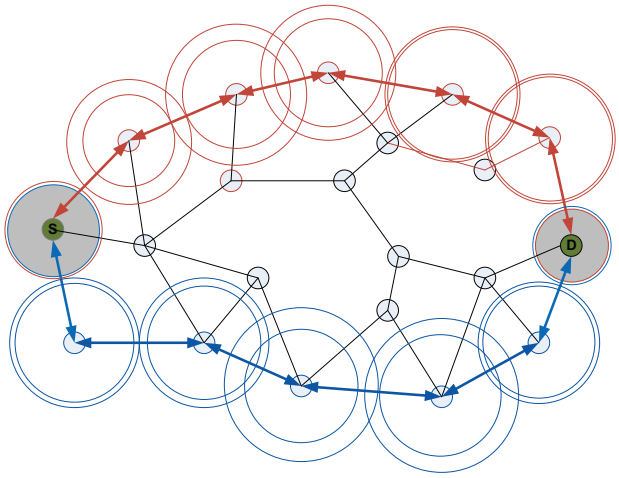

Fig. 3. Multipath Routing and Power Control Approach

C. Non-linear Programming for Optimal Power Assignments

Power assignments performed by the algorithm in Section IV-B are not optimal. It is hard to find optimal power assignments as it requires minimizing an equation of the following form.

$$P_{total} = \frac{C_1}{R_1^n} + \frac{C_2}{R_2^n} + \frac{C_3}{R_3^n} + ... + \frac{C_m}{R_m^n} \quad (5)$$

where m is the number of intermediate nodes on the paths A and B, C_1, C_2,...,C_m are known constants, $n(>= 2)$ is a path loss exponent in the R^n propagation model and R_1, R_2,...,R_m are unknown variables whose values are interdependent and are constrained by equations of the form $R_i + R_j \leq D_{ij}$, where D_{ij} is a known constant. To solve this problem, we use a Non-linear Programming (NLP) formulation for finding optimal (minimum) power assignments for a path pair (A, B) such that conditions 1 and 2 from the section IV-A are satisfied.

V. Reactive Protection against Jamming

Reactive protection against jamming involves computing alternate routes to destination only when a link on the path to the destination fails. In this section, we present a distributed geographic routing algorithm that finds an alternative route to the destination, starting from the first node with failed link on the original path. Both the proactive and reactive techniques ultimately produce geo-diverse source-destination paths, the difference being that in the latter, alternate path computation is initiated only when link failure is detected on the primary path.

A. Link Failure Detection

We assume that every node in a network can detect link failures by performing periodic link maintenance for all neighboring links. Link maintenance is a mechanism by which a node is able to detect whether a neighboring link is functional. There are various ways to perform link maintenance. For example, a node A periodically sends 'Hello Request' packets to a neighbor node B. Node B sends 'Hello Reply' packets to node A for each 'Hello Request' packet received. Node 'A' can monitor link condition (failed or working) based on the 'Hello Request' and 'Hello Reply' packets statistics over a period of time. Link is considered failed if the number of 'Hello Reply' packets received are much less compared to the number of 'Hello Request' packets sent in a given time interval.

B. Algorithm for finding an Alternate Path

A jammer causes collocated link failures in the network. Collection of collocated failed links forms a failed region, called a **jamming void**. The size of a jamming void depends on the type of jamming and the jammer's power. A high power jammer causes a bigger jamming void compared to a low power jammer. Traffic on a path which passes through the jamming void gets disrupted. The algorithm presented in this section discovers a new path to route traffic around the jamming void to the destination. Algorithm 1 computes an alternate path between the first node n with a failed link on the original path, and the destination. A working path from the source to the destination is formed by merging the original path (from the source to the node n) and newly discovered path (from the node n to the destination). Traffic from the source to the destination is routed on the working path until the original path starts working. Algorithm 1 uses $ROUTE\_DIS$ and $ROUTE\_SUC$ packets (Figure 4) for route discovery.

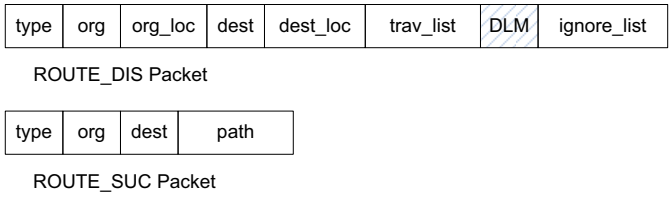

Fig. 4. Algorithm 1 Packets Formats

$ROUTE\_DIS$ packet is created by the node that initiates a route discovery and it is forwarded among network nodes as per the algorithm 1 until a path to the destination is found or until the route discovery fails as the destination is not reachable. $type$ identifies $ROUTE\_DIS$ packet, org contains the node id that initiated the route discovery to the destination, org_loc contains location of the org node, $dest$ contains destination node id for the route discovery, $dest\_loc$ contains location of the $dest$ node, $trav\_list$ is the list of node ids on the path traversed from the org node to a current node which has just received the packet. Node ids that cannot lead to the $dest$ are added to the $ignore\_list$. Nodes in the $ignore\_list$ are not traversed again during the route discovery. $trav\_list$ and $ignore\_list$ are variable size lists. DLM is a special delimiter character which separates $trav\_list$ and $ignore\_list$.

When route discovery succeeds, the destination creates a $ROUTE\_SUC$ packet and sends it to the node which originated the route discovery. org contains node id that created $ROUTE\_SUC$ packet. $type$ identifies $ROUTE\_SUC$ packet. $dest$ contains destination node id for the packet. $path$ is a variable sized list containing node ids on the org to $dest$ path. Table I describes terminology used by algorithm 1.

TABLE I
ALGORITHM 1 TERMINOLOGY

Cur_node_id	Self identity of a node
$Neighbors$	Set containing all active one hop neighbors of a node
$Neighbors\_loc$	Set containing locations of all active one hop neighbors of a node
$Packet$	Packet($ROUTE\_DIS$ or $ROUTE\_SUC$) input to the algorithm
2 * $Path$	If path to the destination is found, algorithm 1 returns $Path$, on the node that initiated route discovery
2 * $FAIL$	If no path to the destination is found, algorithm 1 returns $FAIL$, on the node that initiated route discovery
$NONE$	If there is nothing to return, algorithm 1 returns $NONE$

C. Algorithm for Reactive Protection

Algorithm 1 is a distributed algorithm and it is run on every node in the network. We assume that every node in the network knows its own location as well as the locations of its neighbors. We assume that the node initiating a route discovery knows the location of the destination. Algorithm 1 is invoked when a node initiates route discovery or when a $ROUTE\_DIS$ or $ROUTE\_SUC$ packet is received by the node.

Search performed by the algorithm 1 to reach a destination is essentially like a traversal on a tree which contains all reachable network nodes. Algorithm 1 makes a maximum $2(n-1)$ transmissions in the search process (i.e., traverse at most one path to each node), where n is all network nodes reachable by the originator of the route discovery. Note that choosing the neighbor with the largest *angle* helps to find an alternate geo-diverse path. If the destination is not reachable, then the last transmission of $ROUTE\_DIS$ packet is always for the node which originated the route discovery and $ignore\_list$ of the packet contains all the nodes that are reachable by that node. Information about all reachable nodes is very useful, as a new route discovery for any unreachable node can be avoided within a short time after a failed route discovery.

Algorithm 1 can be embedded into on-demand routing schemes to minimize the number of transmissions required in a route discovery. In on-demand routing schemes, route discovery typically floods the entire network with 'route request' packets. Therefore, performing a flooding based route discovery to find an alternative path for a failed path is very inefficient. On-demand routing schemes can instead use the algorithm 1 to find the alternative path. In most cases,

Algorithm 1 Reactive Protection: Part 1

Input: Cur_node_id, $Neighbors$, $Neighbors\_loc$, $Packet$
Output: One of the following outputs: PATH, FAIL

if $Packet.type == ROUTE\_DISC$ **then**
  if $Packet.dest == Cur\_node\_id$ **then**
    Create $ROUTE\_SUC$ packet
    Search for a neighbor x from $NewPacket.path$
    Remove any nodes between x and Cur_node_id from $NewPacket.path$
    Send $NewPacket$ to node x
  else
    $N \leftarrow Neighbors$ not in ($Packet.ignore\_list$ OR $Packet.trav\_list$)
    if $N ==$ NIL **then**
      if $Packet.org == Cur\_node\_id$ **then**
        Return FAIL
      else
        Remove Cur_node_id from $Packet.trav\_list$, if it exists in the list
        Add Cur_node_id to $Packet.ignore\_list$
        Send $Packet$ to the last node in $Packet.trav\_list$
      end if
    else
      Find a neighbor x from N with highest positive Advance [Advance is the difference of (linear distance between $Packet.dest$ and Cur_node_id) and (linear distance between $Packet.dest$ and neighbor node x)]
      if $x ==$ NIL **then**
        Find neighbor x that makes largest angle between the vector connecting ($Packet.dest, Packet.org$) and the vector connecting ($Packet.dest$,neighbor x)
      end if
      Add Cur_node_id to the end of $Packet.trav\_list$, if not in list
      Send $Packet$ to neighbor x
    end if
  end if

Algorithm 2 Reactive Protection: Part 2

else if $Packet.type == ROUTE\_SUC$ **then**
  if $Packet.dest == Cur\_node\_id$ **then**
    Return $Packet.path$
  else
    Search for a neighbor node x from $Packet.path$
    Remove any nodes between x and Cur_node_id from $Packet.path$
    Send $Packet$ to node x
  end if
end if

Algorithm 1 requires very less number of transmissions in a route discovery compared to a flooding based route discovery mechanism. Evaluation results show that algorithm 1 finds optimal (shortest) paths in most cases.

VI. Evaluations and Results

We evaluate the performance of both the proactive and the reactive approaches to jamming mitigation using extensive OPNET simulations. We present only a representative subset of results due to limited space.

A. Evaluations for Proactive Approach

A grid topology of 81 nodes was used for the OPNET simulations, out of which 10 (source, destination) node pairs were selected for creating uni-directional traffic flows. We compare jamming mitigation effectiveness of three routing approaches under different jamming scenarios. These are: shortest path routing, redundant routing on node disjoint paths and redundant routing on node disjoint paths along with power control on the links of the paths (as described in Section IV). Results from two different scenarios are presented in Fig: 5 and 6 respectively. In the first scenario (Fig: 5), the network contains a stationary jammer on the upper right corner of the grid network while the second scenario (Fig: 6) contains a randomly moving jammer. For both scenarios it can be observed that the proactive approach for power assignment is able to receive all of the traffic sent by the source which is not the case for the other two routing techniques.

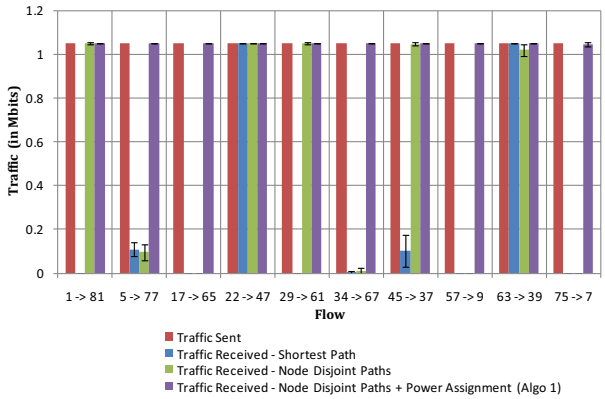

Fig. 5. Grid Topology, Stationary Jammer Near Upper Right Corner of Grid, Jammer's Transmission Power = Node Transmission Power = 0.05 Watt

B. Evaluations for Reactive Approach

We implemented algorithm 1 as a program running on a PC. The program takes network topology, origin node and destination node as inputs, and then runs the algorithm 1 to discover a path from the origin node to the destination node. If a path is found, the program outputs the path from the origin node to the destination node and the number of transmissions required to reach the destination node. We present results of 1 from two different scenarios. In the first scenario (Fig: 7), the network consists of 400 nodes in a grid topology with three partially overlapping jamming voids. The second scenario (Fig: 8) is from a network having a uniform random topology of 400 nodes with three non-overlapping jamming

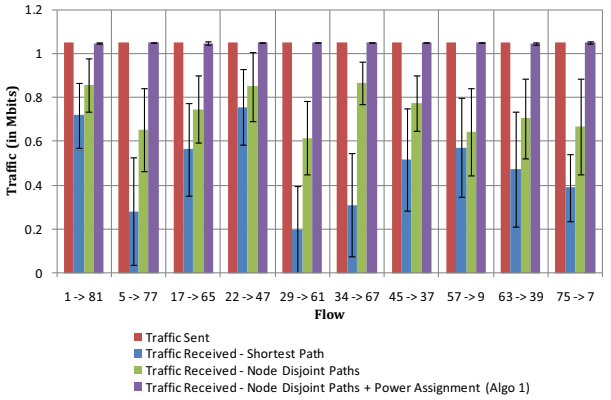

Fig. 6. Grid Topology, Randomly Moving Jammer in the Network, Jammer's Transmission Power = Node Transmission Power = 0.05 Watt

voids. Results from both the scenarios show that paths found from algorithm 1 are nearly optimal (shortest). Although algorithm 1 does lots of backtracking for some path pairs, the total number of transmissions in each case is less than the number of transmissions required for a network wide flooding for route discovery.

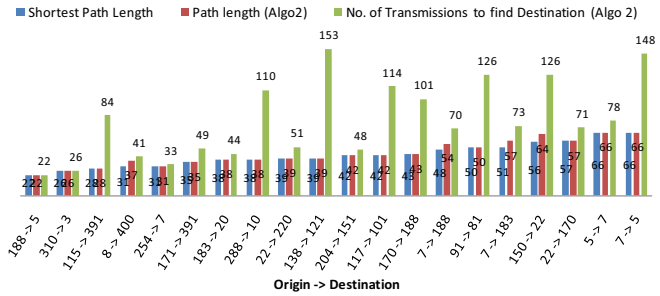

Fig. 7. Algorithm 1 Results for Topology 2

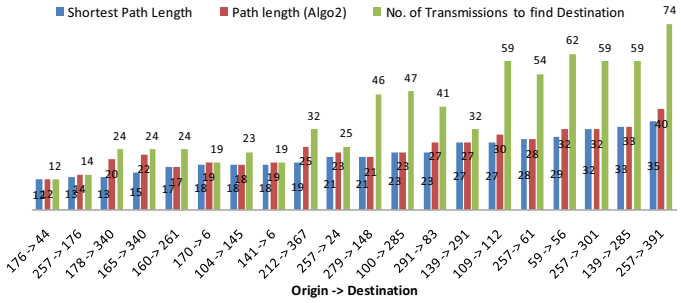

Fig. 8. Algorithm 1 Results for Topology 3

VII. Conclusions

In this work, we have shown that a network layer approach is indeed effective for jamming effects mitigation in wireless multihop networks. We presented a link failure model to represent jamming effects that is pertinent to the network layer. We have shown that routing the traffic redundantly on spatially diverse node disjoint paths is not much effective in defending jamming, unless power control is performed on the links of the paths. We present a proactive and a reactive approach to jamming mitigation, using concepts of geographic routing and redundant multipath routing. The proactive approach performs significantly better than shortest path routing and node disjoint routing without power control. The reactive approach is able to produce paths that are nearly optimal (shortest) in most cases. Our ongoing work includes investigating whether optimal power assignments for proactive protection can be found in polynomial time. For algorithm 1 it may be possible to reduce search time by incorporating limited flooding. Lastly, a combination of proactive and reactive approaches would result in an adaptive algorithm that can dynamically switch between the approaches based on the network's jamming conditions.

References

[1] I. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Computer networks*, vol. 47, no. 4, pp. 445–487, 2005.

[2] R. Bruno, M. Conti, and E. Gregori, "Mesh networks: commodity multihop ad hoc networks," *Communications Magazine, IEEE*, vol. 43, no. 3, pp. 123–131, 2005.

[3] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols," *ACM Trans. Sen. Netw.*, vol. 5, no. 1, pp. 1–38, 2009.

[4] N. Ahmed and H. Huang, "Distributed jammer network: Impact and characterization," in *Military Communications Conference, 2009. MILCOM 2009. IEEE*, 18-21 2009, pp. 1 –6.

[5] T. Karhima, P. Lindroos, M. Hall, and S.-G. Haggman, "A link level study of 802.11b mobile ad-hoc network in military environment," in *Military Communications Conference, 2005. MILCOM 2005. IEEE*, 17-20 2005, pp. 1883 –1886 Vol. 3.

[6] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *Communications Surveys Tutorials, IEEE*, vol. 11, no. 4, pp. 42 –56, fourth 2009.

[7] Y. Ko and N. Vaidya, "Location-aided routing (lar) in mobile ad hoc networks," *Wireless Networks*, vol. 6, no. 4, pp. 307–321, 2000.

[8] Y. Xue and B. Li, "A location-aided power-aware routing protocol in mobile ad hoc networks," in *Global Telecommunications Conference, 2001. GLOBECOM'01. IEEE*, vol. 5. IEEE, 2001, pp. 2837–2841.

[9] M. Mauve, A. Widmer, and H. Hartenstein, "A survey on position-based routing in mobile ad hoc networks," *Network, IEEE*, vol. 15, no. 6, pp. 30–39, 2001.

[10] S. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks," in *Communications, 2001. ICC 2001. IEEE International Conference on*, vol. 10. IEEE, 2001, pp. 3201–3205.

[11] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *MobiHoc '05: Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*. New York, NY, USA: ACM, 2005, pp. 46–57.

[12] D. Thuente, B. Newlin, and M. Acharya, "Jamming vulnerabilities of ieee 802.11 e," in *Military Communications Conference, 2007. MILCOM 2007. IEEE*. IEEE, 2007, pp. 1–7.

[13] A. Wood, J. Stankovic, and S. Son, "JAM: a jammed-area mapping service for sensor networks," in *Real-Time Systems Symposium, 2003. RTSS 2003. 24th IEEE*, 3-5 2003, pp. 286 – 297.

[14] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service," in *WiSe '04: Proceedings of the 3rd ACM workshop on Wireless security*. New York, NY, USA: ACM, 2004, pp. 80–89.

[15] T. Rappaport, *Wireless Communications: Principles and Practice*. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2001.

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