JADE: Jamming-Averse Routing on Cognitive Radio Mesh Networks

(Invited Paper)

Yu Seung Kim, Bruce DeBruhl, and Patrick Tague
Carnegie Mellon University
Email: {yuseungk, bdebruhl, tague}@cmu.edu

***Abstract*—The spectrum sensing capability of cognitive radio (CR) enables a lot of opportunities to wireless networks, but also enables intelligent attacks by malicious players. One attack in this category is reactive jamming, in which the attacker senses the wireless spectrum, decodes parts of packets, and selectively interferes with with packets. In so doing, an attacker can reduce energy expenditure and increase stealth while maintaining a high impact. Of the approaches to mitigate jamming, in this work, we focus on the jamming resilient routing in CR mesh networks. To do this we use signal-to-noise-interference ratio (SINR) which reflects the jamming impact. This metric is difficult to measure with commodity radio chipsets that cannot differentiate jamming interference from the received signal. Detecting SINR becomes even harder if reactive jamming is used by an attacker. In this study, we develop a mechanism to estimate SINR under reactive jamming. The estimated SINR information of each wireless link is then used to determine the jamming-averse directivity (JAD) of packets, which improves the routing performance of the victim network. We validate the proposed mechanism with a simulation study, showing that the proposed JAD escorted (JADE) routing dramatically improves routing path discovery performance including path discovery probability, path length, elapsed time for path discovery, retransmission attempts, and path quality under reactive jamming. Among the 200 route requests at 10 different configurations in our simulation, the reactive jammer disrupts the 77.5% of total requests. However, our JADE routing decreases the route discovery failure rate to 7.5% by saving the 96.7% of failed requests.**

I. Introduction

Our society increasingly depends on wireless connectivity for a multitude of tasks and trends suggest this is going to continue. At any given time and place the wireless spectrum is a scarce resource, made even scarcer by strict government regulations that allow only licensed use of much of the spectrum. Given the scarcity of usable wireless spectrum cognitive radio (CR) as a set of techniques to allow secondary unlicensed users to use the licensed spectrum if it will not interfere with the primary licensed user. One of the key features that make CR possible is spectrum sensing which detects unused spectrum by various scanning algorithms and utilizes the clearest available channel.

Unfortunately, the benefits of spectrum sensing algorithms also can be used by malicious parties to attack wireless networks. An attacker that scans channels usage using spectrum sensing is able to make a significant increase in attack gain such as efficient resource expenditure and harmful impact on target network. For example, a reactive jammer can only broadcast when it detects active communications to save energy and increase stealth [1]. If an attacker has a low-energy multi-channel spectrum sensing technique it could apply this technique to many channels nearly simultaneously with great effect. As techniques for more robust and intelligent communications are developed so are more efficient, stealthy, and devastating attacks. This creates an arms race for control of the wireless spectrum.

One approach to resilient wireless communications is to use cross-layer information from the physical layer to improve routing. We consider a mesh network where paths have been disrupted by jammers aimed at routing. If the attacker is non-adaptive we could use spectral retreat techniques [2] but if the attacker is sufficiently powerful to our CR mesh nodes this will not work. Instead, we propose that each CR node in the mesh network should determine a next hop route which is minimally influenced by interference. One metric to measure the effect of jamming is signal-to-interference-noise ratio (SINR) which can be used to model the probability of correctly receiving a packet. Thus SINR can be used locally by CR mesh nodes determine the next hop candidate with the highest probability of success. The SINR can also be used to determine an optimal routing path over the whole network.

As a matter of fact, measuring SINR at receiver is not a trivial task. To measure SINR for each link between two CR mesh nodes, three measurements are required: signal strength of transmitted signal component at receiver, signal strength of interference component, and noise floor. In a common radio implementation, the three components are not easily differentiable if the jammer generates similar modulated jamming noise at the same frequency. With a naïve constant jamming attack the sum of interference and noise floor can easily be measured which allows us to calculate signal strength of the pure transmitted signal component from measurement of total sum.

Though conceptually easy, in many traditional radio chipsets signal strength is only received during a packet reception making this difficult in practice. In the case of reactive jamming this problem becomes much more difficult. A spectrum measurement when no legitimate signal is sent results in no information about the jamming power level. Instantaneous power measurements during packet reception either consists of all three components or two components (transmitted signal + noise floor) depending on if the jammer has activated yet or

not. We should even consider the case of a jammer which adapts its transmitting power or antenna pattern to further obfuscate matters.

In this paper, we develop an approach to measure SINR at a CR node even when it is attacked by reactive jammers which can selectively respond with legitimate communications. The proposed mechanism uses the exchanged measurements between CR nodes to estimate SINR under jamming. With this SINR estimates, we eventually show how this can be used to improve the routing performance of CR mesh network under jamming. We summarize our contribution in this study as follows.

- We propose a mechanism to estimate the SINR at each CR under the reactive jamming.
- Different from any centralized routing protocol, the proposed jamming-averse routing protocol operates in a distributed manner, thus minimizing the delivery cost of jamming information over entire network.
- Though the simulation results, we validate our scheme can improve the routing performance under jamming.

The rest of this paper is organized as follows. Section II introduces the related work. In Section III, we detail our model assumption throughout this paper. We then present our jamming-averse routing protocol in Section IV. In Section V, we investigate a case that the proposed jamming-averse routing can improve the jamming resilience of an original AODV (Ad Hoc On-Demand Distance Vector) [3] routing and validate its performance through simulation results. We finally conclude the paper in Section VI.

II. Related Work

In general, jamming resilience of network can be regarded as a part of classical network fault tolerance. The key difference in the jamming case, however, is that the failure caused by jamming is emerged across larger number of wireless nodes and wireless links. On the other hand, traditional approaches providing node redundancy or path redundancy commonly assume the failure in locally small groups. Ye et al. propose AODVM [4], which is one of such path redundancy mechanisms for the AODV protocol.

Wood et al. present a mechanism mapping the jammed area that can be used for finding jammer-detouring routing paths [5]. Challenges in the mechanism include the potential congestion around the jammed region and the large amount of time to deliver jamming information over the whole network. Mustafa et al. also propose a path selection protocol utilizing the jamming attack history vector [6]. In the protocol, each node collects the jamming attack history over a period and sends it to a central node. By applying a greedy algorithm the central node selects the best path insusceptible to jamming. Kim et al. propose another jammer-detouring algorithm by providing multiple paths [7] in mesh networks. Assuming that every node knows the geolocations of all nodes in mesh network, the algorithm first divides a network into multiple grids and then finds a path consisting of non-jammed grids between a source and a destination.

In this study, we address the practical difficulty measuring SINR at each link when an attacker uses the advanced reactive jamming. The locally collected SINR information is stored at each node and can be used for the jamming resilient routing. Depending on the given routing protocol, the information needs to be collected at a central node or can be locally used only at each node without global sharing. As a case study, we show how the collected SINR information can be used for AODV without requiring a central decision making node, and high communication costs or computation costs caused by globally sharing information. Moreover, it can relieve a possible concern about the failure of SINR information delivery due to jamming.

III. Model Assumption

A. CR Mesh Network

We assume a mesh network consisting of CR nodes. Each CR node is capable of spectrum sensing, which can not only determine the channel occupancy but recognizes the type of communication by demodulation. Meanwhile, it is also able to change its transmitting power if necessary, but there is a limit constrained by regulation or hardware.

For an ease of analysis, we assume that the antenna gain of all CR nodes is set to 1. In reality, the antenna gain of neighboring nodes as well as itself can be provisioned in advance or delivered through a predefined protocol. If necessary, other information such as the current location of each CR node and the transmitting power can be also shared among CR nodes. Each CR node might be mobile, but in our analysis we assume a stationary configuration for a static analysis. Lastly, in proposing our mechanism throughout this paper, we aim to minimize any redundancy protocol overhead caused by out-of-band messages if possible.

B. Attacker

The attacker's goal is to disrupt the routing operation of CR mesh network and it is achieved by jamming the nearby communication. The jamming device used by the attacker can adjust its transmitting power and has the channel sensing capability since it is based on CR. Instead of constantly transmitting jamming noise, the jammer operates only when it senses the legitimate communication, i.e., reactive jamming [1], [8], [9]. The attacker can recognize the modulation of legitimate communication and transmit the identically modulated jamming noise, and therefore it is practically impossible for the legitimate CR to differentiate the jamming noise from the received signal. The attacker also benefits from this sort of reactive jamming in both reducing resource expenditure and decreasing detectability. Further, the attacker selectively jams the important packets contributing to the routing performance. This type of attack is introduced as *mesh jamming* in our previous study [10], and is regard as an advanced reactive jamming. By jamming only the control packets, not the data packets, the attacker can significantly increase attack gain. Lastly, the attacker may not have full knowledge of geographical configuration of CR mesh network. Therefore, in order

to maximize its jamming impact on routing performance we assume that the attacker uses the omni-directional antenna.

IV. Jamming-Averse Routing

In this section, we present a mechanism to avoid jamming in mesh networks. We first give the definition of jamming-averse directivity (JAD) which is calculated between two adjacent wireless nodes. We consider many different ways to calculate the JAD in various scenarios, and explain how the individual JAD at each link can be used for jamming-averse routing.

A. Jamming-Averse Directivity (JAD)

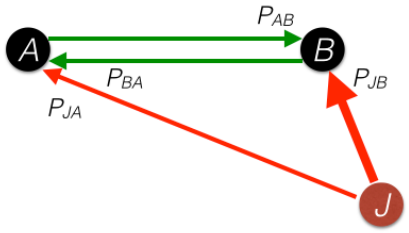


Fig. 1: The two CR node A and B locate near to the jammer J. Since B is closer to J than A, the received jamming signal P_{JB} at B is larger than P_{JA}.

In this section we consider jamming-averse directivity under a constant jamming attack where the attacker always broadcasts. We illustrate this in Fig. 1 where two CR mesh nodes A and B are attempting to communicate while the jammer J broadcasts interference. We can model the total received signal $S_{A|J}$ at A when J when B is not transmitting as

$$S_{A|J} = P_{JA} + N_0, \tag{1}$$

where P_{JA} is the power of received jamming signal at A and N_0 is the ambient noise. When the other CR node B attempts to send a packet to A, the total received signal $S_{A|J,B}$ is

$$S_{A|J,B} = P_{BA} + P_{JA} + N_0, \tag{2}$$

where P_{BA} is the received signal strength of B at A. To estimate which node has a higher probability of successful reception under jamming we compare their SINR estimates. We represent the SINR $\gamma_{A|B,J}$ for a packet from A to B under the jammer J as

$$\gamma_{A|B,J} = \frac{P_{BA}}{P_{JA} + N_0}. \tag{3}$$

Assuming $P_{BA} \approx P_{AB}$ and constant ambient noise then $\gamma_{A|B,J}$ and $\gamma_{B|A,J}$ are differentiated only by P_{JA} and P_{JB}. For example, in Fig. 1, $\gamma_{A|B,J} > \gamma_{B|A,J}$ since $P_{BA} \approx P_{AB}$ and $P_{JA} < P_{JB}$.

As (3) implies, SINR is proportional to the transmitting power at the transceiver. Since a CR node has a capability to change its transmitting power, it is better to know the normalized SINR independent from the current transmitting power. In so doing, we can focus more on the jamming impact at the location of each node regardless of the other CR node's transmitting power. When $P_{BA} \neq P_{AB}$, we thus normalize the SINR values with the transmitting powers at the transceiver. To accomplish this B delivers its transmitting power P_B in packets destined to A, by using the measurements (1) and (2) the normalized SINR $\mathcal{N}$ can be estimated as

$$\mathcal{N}_{A|B,J} = \frac{\gamma_{A|B,J}}{P_B} = \frac{S_{A|J,B} - S_{A|J}}{S_{A|J} \cdot P_B}. \tag{4}$$

Here we define the *jamming-averse directivity* (JAD) with two CR nodes by using their SINR values.

Definition 1. *(Jamming Averse Directivity) For the two CR mesh nodes A and B and jammer J, the jamming averse directivity JAD is defined as*

$$JAD(A,B|J) = \begin{cases} 0, & \text{if } \mathcal{N}_{A|B,J} = \mathcal{N}_{B|A,J} \\ \dfrac{\mathcal{N}_{A|B,J} - \mathcal{N}_{B|A,J}}{|\mathcal{N}_{A|B,J} - \mathcal{N}_{B|A,J}|}, & \text{otherwise.} \end{cases}$$

For example in Fig. 2, $P_{JA} > P_{JB}$ due to the obstacle between B and J. If $P_{AB} = P_{BA}$, then $JAD(A,B|J) = -1$, meaning packets are delivered from A to B under J with higher probability than the opposite direction.

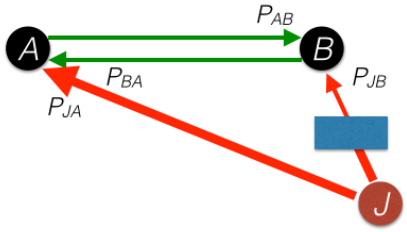


Fig. 2: In this example, although B is closer to J than A, the received jamming signal P_{JA} at A is stronger than P_{JB} due to the obstacle between B and J.

B. JAD Estimation Under Reactive Jamming

Unfortunately, if the jammer use more advanced reactive techniques then measurements like (1) are unavailable. We consider alternatives to direct passive measurement.

1) Transmitting with equal power: If $P_A = P_B$ and the wireless channel between the two nodes is reciprocal, $P_{AB} = P_{BA}$. In this case, JAD can be calculated by using the measurement (2) as

$$JAD(A,B|J) = \frac{P_{JB} - P_{JA}}{|P_{JB} - P_{JA}|} = \frac{S_{B|A,J} - S_{A|B,J}}{|S_{B|A,J} - S_{A|B,J}|} \tag{5}$$

2) Estimating received signal strength using location information: In the case that the transmitting powers of two CR nodes are different, the received signal strength needs to be estimated. Specifically, if A receives a packet containing P_B from B and it knows the distance between A and B, it can

estimate P_{BA}. Depending on the given configuration, different channel fading model can be used. For instance, according to the Friis transmission equation, P_{BA} is estimated as

$$\widehat{P_{BA}} = P_B G_A G_B \left(\frac{1}{4\pi}\right)^2 \left(\frac{\lambda}{d_{AB}}\right)^n, \quad (6)$$

where G_A is the antenna gain at A to the direction of the opposite node, λ is the wavelength, d_{AB} is the distance between the two nodes, and n is the loss exponent, which varies with the given geographical configuration [11]. With the estimated received signal strength, JAD is computed as

$$\begin{aligned} JAD(A,B|J) &= \frac{P_{JB} - P_{JA}}{|P_{JB} - P_{JA}|} \\ &= \frac{(S_{B|A,J} - \widehat{P_{AB}} + (S_{A|B,J} - \widehat{P_{BA}})}{|(S_{B|A,J} - \widehat{P_{AB}} + (S_{A|B,J} - \widehat{P_{BA}})|} \end{aligned} \quad (7)$$

3) Bait-and-switch measurement: In the case of a highly configurable radio we could also consider a bait-and-switch approach to measuring (1). Reactive jamming often works by broadcasting after a preamble is detected or after a header is decoded and it is determined this packet is of interest [9]. Because of this node A can broadcast the preamble or the preamble and header to a packet and then switch to listening and directly measure the power when the attacker broadcasts which should cause a spike in the spectrum. We illustrate both reactive jamming and the bait-and-switch technique to measure jamming power levels in Fig. 3.

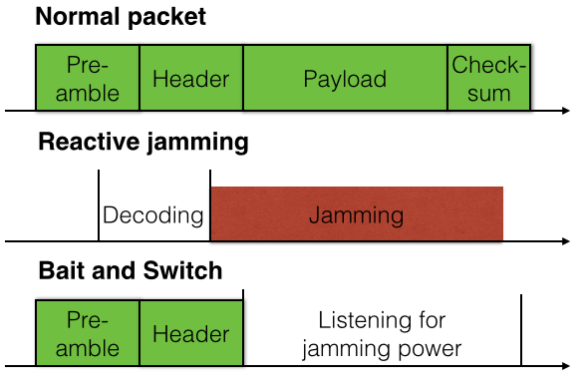


Fig. 3: In this figure we show an example of reactive jamming which makes it difficult to measure interference power levels. We also show our proposed bait-and-switch technique to get the jammer to broadcast and allow us to measure its power.

C. JAD Escorted (JADE) Routing

Since the jammer selectively jams the routing packets, the JAD should be managed per each routing packet type. The procedure of calculating the JAD between two nodes A and B is summarized as follows.

1) A sends out a routing packet containing its transmitting power P_A.
2) B overhears the packet sent from A, and records the total received signal strength and P_A embedded in the packet. If the SINR of the packet at B is lower than the SINR threshold so that it cannot be decoded at B, it uses the predefined P_A. If P_A is not fixed, B reads it from another type of packet from A.
3) B exchanges its recorded observations about A with A.
4) If it is necessary, B uses the distance between A and B to estimate P_{AB}.
5) Based on the received observation from A, B calculates the JAD.

Note that this procedure is identical as well for the opposite direction, i.e., when A hears B. Also this procedure should be executed per each type of routing packet, meaning that JAD is collected per link per packet type. The calculated JAD information is stored at each node during a given time period, since the jammer can change its attacking strategy (e.g., transmitting power and location).

The JAD information at each node can be utilized in many different ways depending on the type of routing protocol used in the given CR mesh network. If, for example, the routing decision is made in a central node, the JAD information at all nodes should be delivered to the node. However, for many reasons this method is not recommended.

- The jammer can also selectively disrupt the delivery of JAD information.
- Even though the JAD information is collected in a distributed manner, the delivery process to the central node can be very inefficient in terms of network bandwidth, resource expenditure, and time.
- The centralized routing itself is vulnerable to the attack since it has a point of failure.

We thus focus more on the ad-hoc style distributed routing protocol which does not depend on a central point to benefit from the JAD information. In ad hoc routing protocols such as OLSR [12], BATMAN [13], and AODV [3], the JAD information stored at each node is contained in the routing packets and used as a link quality indicator. The JAD information can replace the previous link quality measure or be combined to the existing ones under the jamming situation.

In Fig. 4, a CR mesh network consisting of 50 nodes jammed by the two jammers $j1$ and $j2$ is depicted. The wireless link between two nodes is drawn as a green line. The arrow in each line represents the JAD, i.e., packets can be better delivered to the direction of arrow than the opposite direction. The purple line means the opposite direction of arrow is currently jammed, so packets cannot be delivered. At the link colored in red, packets are not delivered to any directions.

Although the JAD information is stored at each CR node, it is in fact a value assigned to each individual link. Since it represents only the direction to the less likely jammed node between two nodes, it is hard to accurately reflect the jamming impact at the distant area. This brings us to develop another metric implying the proximity to jammers. Intuitively, the

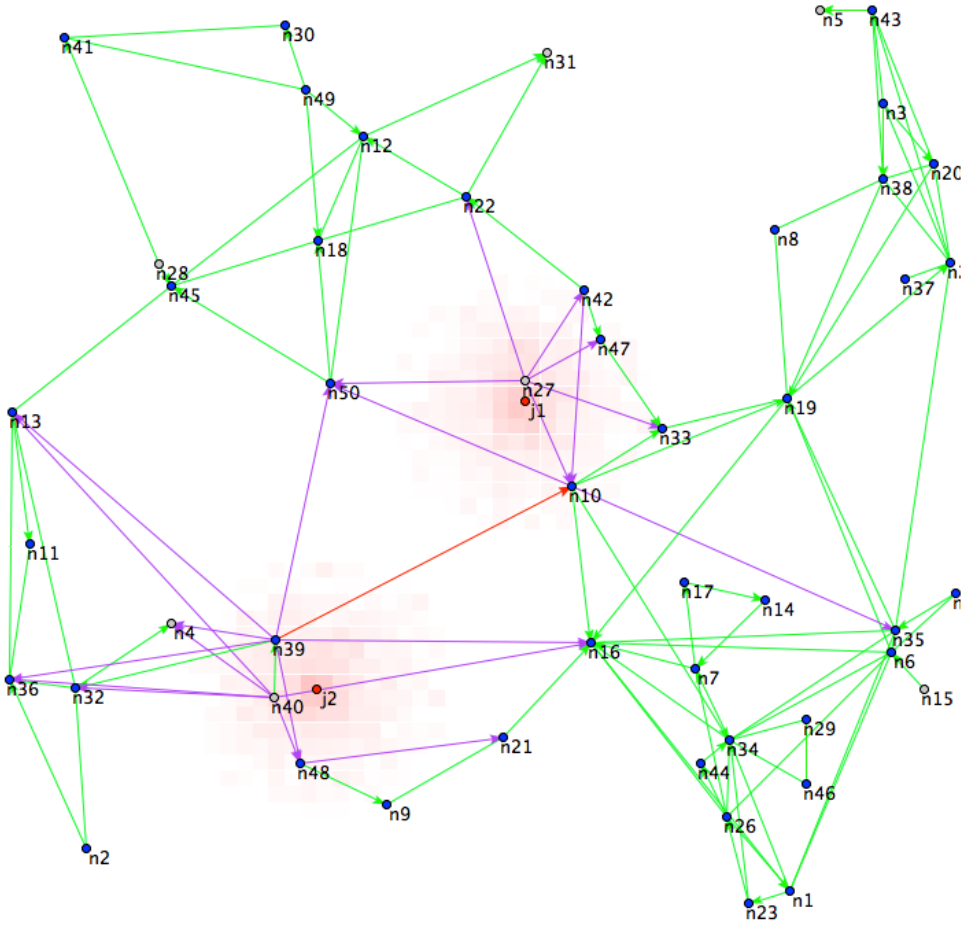


Fig. 4: A mesh network of 50 CR nodes jammed by two jammers $j1$ and $j2$ is shown. The JAD information at each link is shown as an arrow of each line. The lines without an arrow mean that there is no directivity ($JAD = 0$).

node close to the jammer has the JAD of -1 to its neighbors, while the node in-between multiple jammers has the JAD of 1. Both these types of nodes should be avoided for routing since it is difficult for them to receive packets or to forward the received packets to other neighbors. Thus we define the following metric per node basis.

Definition 2. *(Directivity Circular Level) For a CR node A and its neighbor $N \in \mathbb{N}$, the directivity circular level DCL of A is defined as*

$$DCL(A) = \left| \frac{\sum_i JAD(A, N_i|J)}{\|\mathbb{N}\|} \right|.$$

In Fig. 4, the CR nodes which of DCL is equal to 1 are shown as gray circles (e.g., $n4$, $n5$, $n15$, $n27$, $n28$, $n31$, $n40$). There is a high correlation between the DCL of node and the proximity to the jammers (e.g., $n4$, $n27$, and $n40$). The other exceptional nodes usually have a few number of neighbors at the edge of network.

V. Case Study: AODV

In this section, we show how the JAD information can be combined with the existing ad hoc routing protocols to defend against reactive jamming. Among many different types of ad hoc routing protocols, we choose the AODV routing protocol as a case study. The AODV is one of widespread routing protocols with the efficient resource expenditure owing to its reactive nature. It is also used as a mandatory part of the IEEE 802.11s mesh networking standard [14]. In our previous study [10], we investigated the impact of reactive jamming in IEEE 802.11s mesh networks and found that an attacker can significantly improve its attacking gain by selectively jamming only PREP (path reply) frames. In the following, we first explain how the JADE routing can improve the routing performance against the PREP jamming. We provide the description of simulation setup and present the routing performance results.

A. Applying JADE Routing to AODV

Fig. 5a and Fig. 5b show the principle of the PREP jammer to disrupt the routing path discovery. In AODV, the PREQ

packets are broadcast over the whole network and the link quality in each link is accumulated as the PREQ packets are forwarded at each node. The destination node receiving the PREQ packets via multiple paths selects the minimum cost path based on the accumulated link quality embedded in each PREQ packets. In this example in Fig. 5a, the path $n_1 \rightarrow n_2 \rightarrow n_3 \rightarrow n_4 \rightarrow n_6$ is selected as the minimum cost path at n_6. The node n_6 replies to n_1 with the PREP packet along the chosen path, but it cannot be delivered at the link $n_4 \rightarrow n_3$ due to the jammer J jamming only the PREP packet as shown in Fig 5b.

To cope with the reactive jammer J, we apply the JADE routing to the existing AODV protocol. First, each node calculates the JAD by observing the neighboring node's communication. Based on the JAD, each node also calculates the DCL value as shown in Fig. 5c. If a CR node has the DCL value higher than a threshold, it is regarded as a jammed node. In this example, we set the threshold to 1. The CR nodes determined to be jammed do not forward the received PREQ or forward it with setting a poor link quality value, thus being penalized at the destination. As a consequence, the path $n_1 \rightarrow n_2 \rightarrow n_4 \rightarrow n_6$ is selected as the best at n_6, and the PREP is successfully delivered along the chosen path as illustrated in Fig. 5d.

B. Simulation Setup

In order to extensively validate the JADE routing in the AODV, we use a simulation on the on-demand part of IEEE 802.11s standard (i.e., AODV). The simulation is based on the line-of-sight (LOS) signal propagation model [15], the loss exponent is set to 2.4, and the operating frequency is 2.4 GHz ISM band. The antenna gain of all devices in the simulation is set to 1. The simulation model follows the standard IEEE 802.11g parameters for rate adaptation technique deepening on the SINR. For transmitting unicast frames (PREP), each node retransmits 7 times at maximum if it does not hear ACK from the receiver. We set the clear channel assessment (CCA) threshold to -82 dBm, and the ambient noise is set to -95 dBm.

Over the 600x600 square meters of area, 50 CR nodes are randomly placed with the transmitting power ranging from 0 dBm to 20 dBm. The wireless link between nodes are determined by their ability to exchange the packets, i.e., sufficient transmitting power for the given relative distance between nodes (minimum SINR threshold = 18 dB). In the mesh network, there are two independent path requests are triggered at random nodes at random time. We also install the two jammers with a random power, which jam only the PREP packets in the vicinity. We generate the 10 different mesh network configurations, and repeat the simulation 10 times in each configuration.

C. JADE Routing Performance

To quantitatively compare the performance of JADE routing to the existing AODV under jamming, we use the following metrics.

- ϵ_{pd}: the probability that a path discovery succeeds.
- δ_{pl}: the ratio of the length of discovered path with the JADE routing over one with the original AODV. This metric is calculated only when the path is discovered in both cases.
- δ_{et}: the ratio of the elapsed time spent for discovering path with the JADE routing over one with the original AODV. This metric is calculated only with the path is discovered in both bases.
- δ_{rt}: the ratio of the retransmission attempt during the path discovery with the JADE routing over one with the original AODV. This metric is calculated only with the path is discovered in both bases.
- δ_{pq}: the path quality is calculated by multiplying all the link qualities along the discovered path. This metric is calculated by subtracting the path quality with the original AODV from one with the JADE routing.

Fig. 6 shows the performance of JADE routing under jamming through these metrics. As shown in Fig. 6a, in most cases (except for the first path in the configuration #8) the JADE routing successfully discovers the path under the impact of PREP jammer. Among the 200 routing requests at 10 different configurations in total, the reactive jammer fails 155 requests and the JADE routing recovers the 140 requests (about 96.7% of failed requests). In the configuration #8, the path request for the first path always passes through the jammed region, and thus no detouring path exists. As represented in Fig. 6d, the JADE routing attempts a lot of retransmission to find a detouring path. Overall, the JADE routing shows a slight increase in some cases in terms of the path length, the elapsed path discovery time, the retransmission attempts, and the path quality. However, it is very promising that it apparently improves the path discovery ability of mesh network under jamming by sacrificing a small overhead.

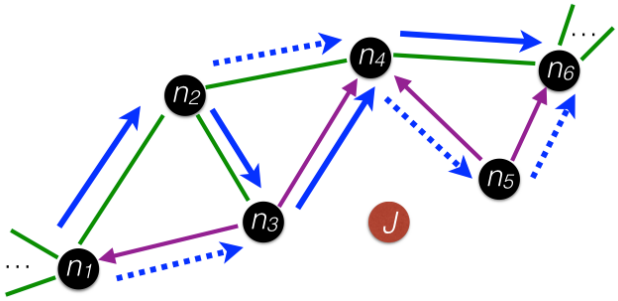
VI. Conclusion

In this paper, we presented a mechanism to estimate SINR under various reactive jamming attacks. We use these SINR estimates to define *jamming-averse directivity (JAD)* of the wireless link between nodes, and showed that the JAD can be extended to define the *directivity circular level (DCL)* to imply the packet forwarding probability under jamming attacks. Through extensive simulations, we validate that the proposed routing mechanism *(JADE)* significantly recover the degraded routing performance metrics including path discovery probability, path length, elapsed time for path discovery, retransmission attempts, and path quality under reactive jamming.

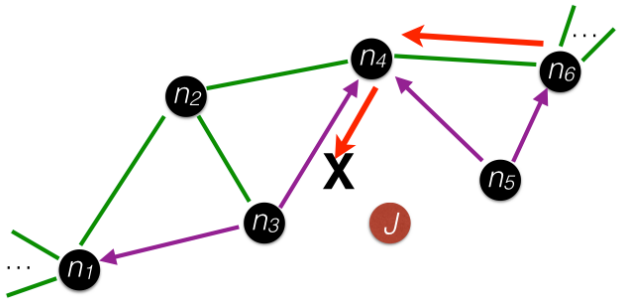
References

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

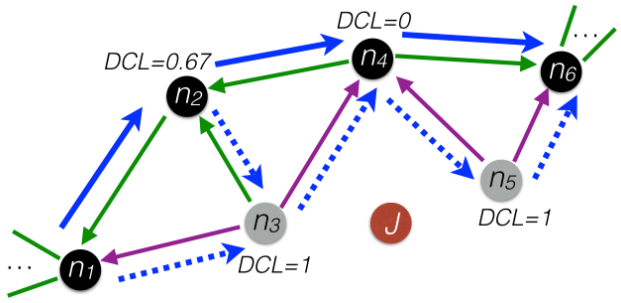
[2] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: Defenses against wireless denial of service," in *Proceedings of the 3rd ACM workshop on Wireless security (WiSe '04)*, 2004.



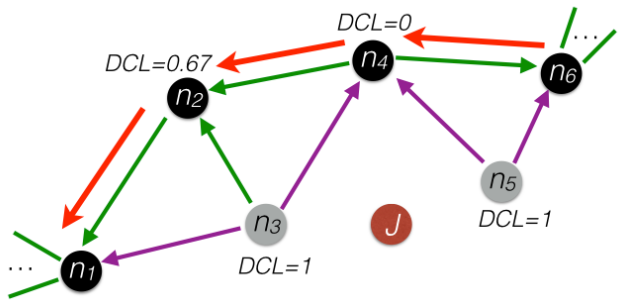
(a) PREQ propagation: a routing path to n_6 is requested at n_1 and accordingly path request (PREQ) packets are broadcast over the whole network. The blue arrows show the propagation of PREQ and the blue solid arrows represent the links belonging to the minimum cost path.



(b) PREP delivery: after receiving PREQ at n_6, path reply (PREP) sent back to n_1 along the selected best path ($n_6 \rightarrow n_4 \rightarrow n_3 \rightarrow n_2 \rightarrow n_1$). However, it cannot be delivered at the link between n_4 and n_3 due to J.



(c) PREQ propagation with JADE routing: each node calculates the JAD and it is shown as the green arrow. Integrating the JADs of all links, each node also calculates the DCL. The two gray nodes n_3 and n_5 show the high DCL value, so they are excluded in the path discovery. Thus the minimum cost path is selected along the nodes n_1, n_2, n_4, and n_6.



(d) PREP delivery with JADE routing: PREP is successfully delivered to n_1 along the path not jammed by J.

Fig. 5: Shown are the JADE routing procedure in a mesh network using AODV. A mesh network consists of CR nodes $n_1 \sim n_6$ and the jammer J selectively jams PREP (path reply) packets. Due to jamming impact, PREP cannot be delivered along the opposite direction of purple arrows, while it can be bidirectionally delivered over green lines.

[3] C. Perkins, E. Belding-Royer, S. Das *et al.*, "RFC 3561-ad hoc on-demand distance vector (AODV) routing," *Internet RFCs*, pp. 1–38, 2003.

[4] 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, Mar.-Apr. 2003, pp. 270–280 vol.1.

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

[6] H. A. Mustafa, X. Zhang, Z. Liu, W. Xu, and A. Perrig, "Short paper: Jamming-resilient multipath routing leveraging availability-based correlation," in *Proceedings of the fourth ACM conference on Wireless network security*, ser. WiSec '11. New York, NY, USA: ACM, 2011, pp. 41–46. [Online]. Available: http://doi.acm.org/10.1145/1998412.1998421

[7] M. Kim and K. Chae, "Dmp: Detouring using multiple paths against jamming attack for ubiquitous networking system," *Sensors*, vol. 10, no. 4, pp. 3626–3640, 2010.

[8] A. Proano and L. Lazos, "Packet-hiding methods for preventing selective jamming attacks," *Dependable and Secure Computing, IEEE Transactions on*, vol. 9, no. 1, pp. 101–114, Jan.-Feb. 2012.

[9] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short paper: reactive jamming in wireless networks: how realistic is the threat?" in *Proceedings of the fourth ACM conference on Wireless network security*, ser. WiSec '11. New York, NY, USA: ACM, 2011, pp. 47–52.

[10] Y. S. Kim, B. DeBruhl, and P. Tague, "Meshjam: Intelligent jamming attack and defense in ieee 802.11 s wireless mesh networks," in *Mobile Ad-Hoc and Sensor Systems (MASS), 2013 IEEE 10th International Conference on*. IEEE, 2013, pp. 560–564.

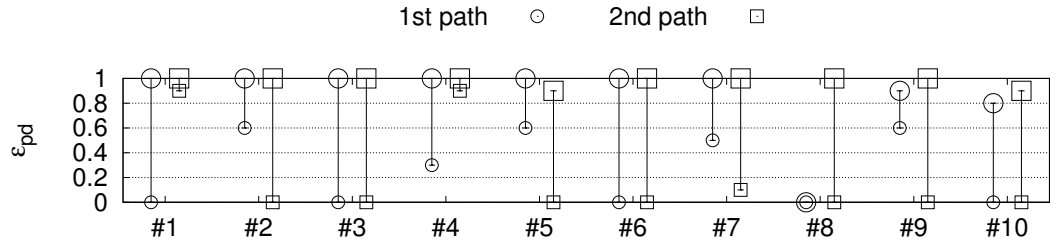
[11] R. A. Poisel, *Introdunction to Communication Electronics Warfare Systems*. Artech House, Inc., 2002, ch. 2, pp. 27–33.

[12] T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, and L. Viennot, "Optimized Link State Routing Protocol (OLSR)," 2003, network Working Group Network Working Group. [Online]. Available: http://hal.inria.fr/inria-00471712

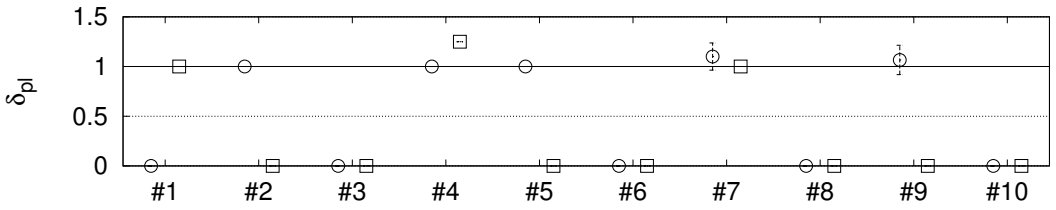
[13] D. Johnson, N. Ntlatlapa, and C. Aichele, "Simple pragmatic approach to mesh routing using batman," 2008.

[14] *IEEE Std 802.11s-2011, Amendment 10: Mesh Networking*, IEEE Computer Society Std.

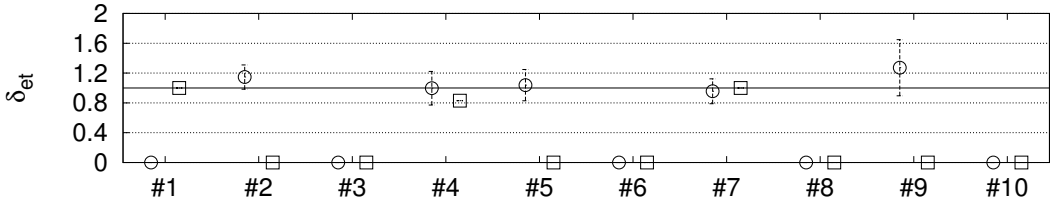
[15] R. A. Poisel, *Modern Communications Jamming Principles and Techniques*. Artech House, Inc., 2004, ch. 2.



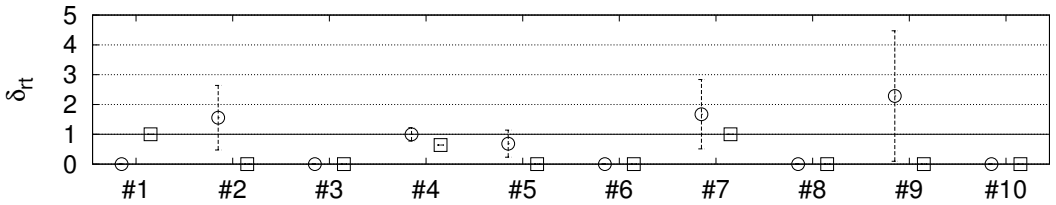
(a) Path discovery probability change - bigger markers are ϵ_{pd} after applying JADE routing.



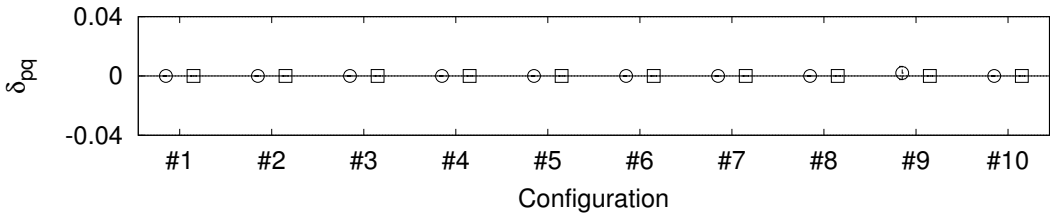
(b) Path length expansion - smaller values of δ_{pl} than 1 indicate that the defense mitigates the jamming effect.



(c) Elapsed time expansion - smaller values of δ_{et} than 1 indicate that the defense mitigates the jamming effect.



(d) Retransmission number expansion - smaller values of δ_{rt} than 1 indicate that the defense mitigates the jamming effect.



(e) Path quality expansion - larger values of δ_{pq} than 0 indicate that the defense mitigates the jamming effect.

Fig. 6: Performance of JADE routing under jamming at 10 different configurations. The error bar is defined as $(m \pm \sigma)$. For an easy presentation, the value of NaN is also plotted as 0.