On Adjusting Power to Defend Wireless Networks from Jamming

Wenyuan Xu
Department of Computer Science and Engineering
University of South Carolina, Columbia, SC 29208
Email: {wyxu}@engr.sc.edu

***Abstract*— Wireless networks are susceptible to accidental or intentional radio interference. One way to cope with this threat is to have the radios compete with the jammer, whereby the network nodes adapt their transmission power to improve the chance for successful communication. In this paper, we examine issues associated with using power control both theoretically and experimentally. We begin by examining the two-party, single-jammer scenario, where we explore the underlying communication theory associated with jamming. We note that the effect of the jammer upon source-receiver communications is not isotropic. We then discuss the potential for improving communication reliability through experiments conducted using Mica2 motes, and in particular explore the feasibility of power-control for competing against jammers. Next, we turn to examining the more complicated scenario consisting of a multi-hop wireless network. We show the complex jamming effect by applying the non-isotropic model of jamming to a multi-hop wireless network, and it is necessary to have a feed-back based power control protocol to compete with jamming interference.**

I. Introduction

Technological advancements have caused wireless networks to become commoditized. As a consequence, there are many types of wireless networks being deployed for a variety of different purposes. Wireless Local Area Networks (WLANs) are now a common form of access network, and methods for extending the coverage of WLANs through multi-hop protocols have led to several successful deployments of ad hoc or mesh networks. Sensor networks, which also use light-weight radio technologies in conjunction with multi-hop protocols, are gaining acceptance for the continual monitoring of a broad array of events. Whether one considers WLANs, mesh networks, or sensor networks, the reliable operation of a wireless network is closely tied to the ability of wireless devices to successfully communicate with each other. One challenge facing wireless networks, though, is the fact that successful communication across a wireless network can be severely disrupted by radio interference.

Whether intentional or not, interference and jamming is a serious threat to the reliable communication of wireless messages. The traditional approach to coping with radio interference is to employ more sophisticated physical-layer technologies (such as spread spectrum). Such methods, however, imply more expensive transceivers and, with the exception of some military systems, most commodity wireless networks do not employ sufficiently strong spreading techniques to survive jamming or to achieve multiple access. In fact, conventional physical layer anti-jamming methods are currently not economically conducive to the commoditization of wireless technologies, and therefore other alternatives that are suitable for conventional off-the-shelf wireless platforms are desirable.

Recent studies [1]–[3] have presented several evasion strategies, whereby wireless nodes try to evade jamming/interference either in the spectral sense or in the geographical sense. In this paper, however, we explore an alternative approach to coping with jamming– wireless devices should attempt to compete against the jammer rather than escape from the jammer. Specifically, we examine the possibility of using power control to compete against jamming attacks, both at the local communication level as well as across a multi-hop wireless network. Wireless nodes, upon detecting the presence of a jamming attack [4], attempt to overcome the effect of the interference by adjusting their transmission power levels. In order to thoroughly analyze the effectiveness of power control methods for defending wireless networks from radio interference, we have studied the issues from both the adversary side and the defense side.

We begin the paper in Section II by examining the theory relating power levels to the ability of a pair of communicators to effectively communicate in the presence of a jammer. Additionally, we explore a geometric model for the effect of a jammer upon source-receiver communications, noting that the effect of a jammer is non-isotropic (as opposed to the common circular model for jamming) and depends on location as well as source and jammer transmission power. In order to complement the underlying theory, we present experimental results in Section III by showing how such theoretical results manifest themselves in practice. Based on these results, we identify conditions for the local two-party communication scenario where it is possible to compete with a jammer by adjusting the sender's transmit power. We then move to the more general case of multi-hop wireless networks in Section IV, where we explore the complexity involved in tuning up the transmission power. We wrap up the paper by discussing related work in Section V, and provide concluding remarks in Section VI.

II. Theoretical Models for the Effect of Jamming

We now explore two different aspects for modeling the effect of a jammer on communication effectiveness: first, we evaluate the effect of jamming in terms of its effect on the channel capacity between a sender and a receiver; and, second, we provide a geometric model describing a

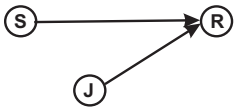


Fig. 1. Two-party radio communication scenario.

relationship between the effect of a jammer and both the location and transmission powers of the participants.

A. Effect of Jamming in Channel Capacity

We start by first examining the theoretical underpinnings of tuning transmission power to cope with jamming attacks. Let's consider a simple network consisting of a source S, a receiver node R, and a jammer J that is interfering (either intentionally or accidentally) with legitimate wireless communications between S and R, as depicted in Figure 1. The jammer J can achieve this goal by either proactively jamming the channel or reactively adjusting its jamming strategy based on the communication J observes. We will describe the jamming strategies in Section II-B. In this section, we focus our discussion on a proactive jammer, where the jammer continuously send out an interference signal. Additionally, we assume the channel between node S and node R, jammer J and node R are both additive white Gaussian noise (AWGN) channels.

For simplicity, we shall abuse notation and let S be the signal sent by the sender S and J the one blasted by the jammer J. We assume that our signals are transmitted over a channel with bandwidth B. Without loss of generality, we assume the channel response for both the sender and the jammer is frequency non-selective (i.e. constant). This allows us to absorb the role of the $S \rightarrow R$ and $J \rightarrow R$ channel amplitude responses into the transmit power of S and J respectively, so that the received signal at node R is:

$$R = S + J + N, \tag{1}$$

where N is the Gaussian noise with variance σ^2, the signal S has power $P_s = 2B\sigma_s^2$ and the signal J has power $P_j = 2B\sigma_j^2$. The capacity of the communication channel between node S and node R is formally defined as

$$C = \max_{p(s)} I(S;R), \tag{2}$$

where $I(S;R)$ is the average mutual information that can be inferred about the transmitted signal S by observing the received signal R. The capacity of the channel, which is the maximum bit rate from $S \rightarrow R$, is the maximum value of $I(S;R)$ over all input symbol probability distributions. It is well-known that $I(S;R)$ is maximum when S is a Gaussian random variable [5], which is parameterized by the variance (power) term σ_s^2. Therefore, we shall assume that the sender's transmitted signal is a zero-mean Gaussian signal. Similarly, we also assume that the jammer employs an optimal interference strategy, so that J's signal is a zero-mean Gaussian random variable with power σ_j^2. Straight-forward calculations give that the channel capacity as

$$C = \max_{p(s)} I(S;R) = B\log_2(1 + \frac{2\sigma_s^2}{2\sigma_j^2 + 2\sigma^2}). \tag{3}$$

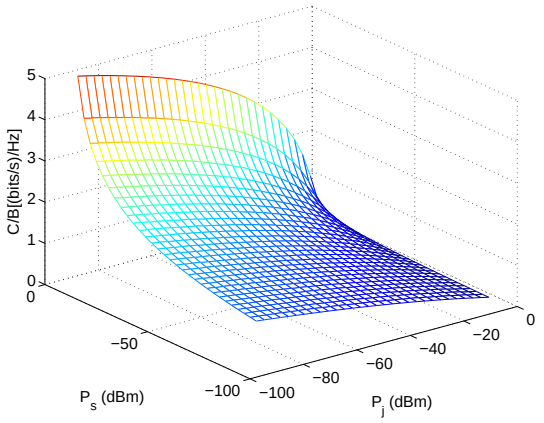


Fig. 2. Normalized channel capacity as a function of P_s and P_j.

In the case where the noise power is much smaller than the jamming power, the channel capacity is approximately

$$C = B\log_2(1 + \frac{P_s}{P_j}) \tag{4}$$

where P_s is the average transmission power of signal S, P_j is the average transmission power of jamming signal J. We plot the normalized capacity C/B versus the signal power P_s and the jamming power P_j in Figure 2. For a given jamming power and bandwidth B, as the signal power P_s increases, the channel capacity increases, which suggests that increasing the transmission power P_s is a feasible method to overcome a given jamming power P_j as it increases the channel capacity.

B. Non-isotropic Model for Jamming

We now provide a geographical interpretation of the effect of jamming on the effectiveness of wireless communications. Typically, most recent papers on jamming and wireless networks have modeled the effect of the jammer as an isotropic effect. This has caused many authors to depict the effect of a jammer as a circular region that is centered at the jammer's location. In reality, though, such an interpretation of jamming is overly simplistic and does not provide a complete depiction of the complex relationships between source and jammer transmit power, and the geometry of the deployment.

The circular jamming model does not capture the fact that the success reception of a packet is primarily determined by S/J at the receiver R. This ratio depends on multiple factors, including the transmitter and jammer power, as well as the distances between the receiver R and the source S and the jammer J, i.e. d_{SR} and d_{JR}.

For a given pair of source S and jammer J locations, changing the location of the receiver R amounts to changing d_{SR} and d_{JR}, which in turn result in different ratios $\gamma_{S/J}$. To better understand the effectiveness of the jammer, we now derive the contours of constant $\gamma_{S/J}$.

Let us use the standard free-space propagation loss model. In this case, the received power is

$$P_R = \frac{P_T G_T G_R}{4\pi(d/d_0)^2} \tag{5}$$

where, P_T is the transmission power of a transmitter; G_T is the antenna gain of that transmitter in the direction of

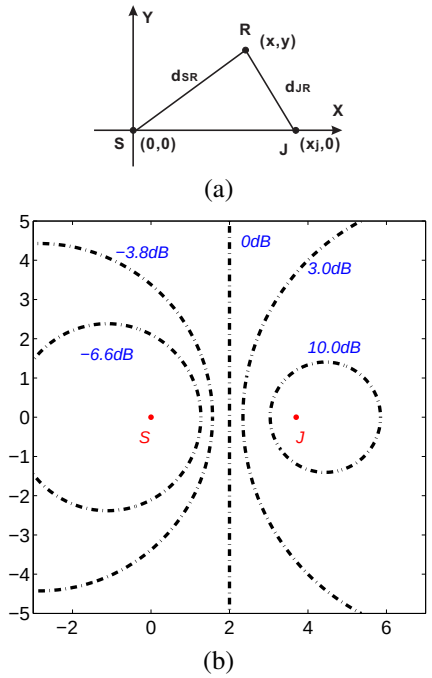


Fig. 3. Coordinate system for constant S/J contours, (a) the positions of the sender S, the receiver R, and the jammer J; (b) constant S/J contour plot, where the distance between S and J is 4 units. The contour labels are the ratio of P_{ST}/P_{JT}, and the contour lines correspond to the edge where $\gamma_{S/J} = 0dB$.

the receiver; G_R is the antenna gain of the receiver in the direction of the transmitter. d is the distance between the transmitter and the receiver, while d_0 is a reference distance (typically chosen so that $d_0 = 1$). When applying this signal propagation model to the jamming problem, we apply it to both the sender as well as the jammer. Assuming that the jammer uses the same type of device as the sender, e.g. both use omni-directional antennas, then the antenna gains G_T of the sender and the jammer are the same in all directions.

The signal-to-interference ratio at the receiver thus becomes

$$\gamma_{S/J} = \frac{P_{SR}}{P_{JR}} = \frac{P_{ST} d_{JR}^2}{P_{JT} d_{SR}^2}. \quad (6)$$

Where P_{ST} is the transmission power of the sender S, P_{JT} is the transmission power of J. In the coordinate system shown in Figure 3, the sender S is placed at the origin $(0, 0)$, the jammer J is located at $(x_j, 0)$, and the receiver R is arbitrarily placed at (x, y). Noting that $d_{SR}^2 = (x_j - x)^2 + y^2$, and $d_{JR}^2 = x^2 + y^2$, we may substitute to get the contours of constant $\gamma_{S/J}$

$$(x - \frac{x_j}{1-\beta})^2 + y^2 = \frac{\beta x_j^2}{(1-\beta)^2}, \quad (7)$$

where $\beta = \frac{\gamma_{S/J}}{P_{ST}/P_{JT}}$. For a given P_{ST} and P_{JT}, the constant contours of $\gamma_{S/J}$ are circles centered at $(\frac{x_j}{1-\beta}, 0)$ with radius $\frac{\sqrt{\beta} x_j}{|1-\beta|}$.

We provide a depiction of equation (7) in Figure 3 (b). In this figure, we provide several contours corresponding to different transmit signal-to-jamming ratios, i.e. $P_{ST}/P_{JT} \in \{-6.6, -3.8, 0, 3.0, 10.0\}$ dB. Each of these contours map out loci of constant received signal-to-interference ratio corresponding $\gamma_{S/R} = 0dB$. We now discuss the interpretation of this figure. First, we note that the case $P_{ST}/P_{JT} = 0$dB splits the figure into two separate categories of curves: those centered near the source and those centered near the jammer. First, for those centered near the source, we may interpret these regions as areas where, if we were to place a receiver within one of these contours, it would be able to successfully decode transmissions from the source if the required signal-to-jammer ratio is $\gamma_{S/R} = 0dB$. Hence, a receiver located within the $P_{ST}/P_{JT} = -6.6$dB curve, would be able to decode packets (i.e. the receive signal-to-interference level would be better than 0dB) from a source that is transmitting at a level 6.6dB below the jammer. On the otherhand, the circles centered near the jammer imply the contrary– a receiver within one of these circles would receive packets at a signal-to-interference level *worse* than $\gamma_{S/R} = 0dB$. For example, for those locations within the $P_{ST}/P_{JT} = 10$dB curve, even though the source transmits at a level 10dB higher than the jammer, the receiver is still unable to decode the transmission.

For both cases, however, we note that the effect of increasing the sender's transmit power is the same. At a given jammer transmission power, increasing the transmission power of the sender decreases the area where the $\gamma_{S/J}$ is smaller than $0dB$. This corresponds to decreasing the effective jammed area. We note that, in a realistic deployment, the contours will not be so regular, due to the non-uniformity of the underlying multipath propagation environment.

III. Experimental Evaluation

The relationship describing the effect of a jammer upon the channel capacity is a theoretical result that only describes the effect of source and jammer power levels upon the potential for the resulting communication channel to support communications. In reality, however, there are many other systems issues that impact the performance of practical communication systems. For example, it is well known that the relationship between signal to noise ratio and the reliability of a communication link does not follow the smooth $log(1 + SNR)$ capacity curve that theory describes, but in fact typically follows a brickwall-shaped curve where the communication link suddenly fails after falling below a threshold SNR level.

In this section, we provide an systems-level exploration of the relationship between sender transmission power, jammer transmission power, and the locations of the communication participants. Based on this study, we also assess the feasibility of increasing transmission power to repair local network connectivity in the presence of jamming.

A. Experiment Setup

In our experiment, we used MICA2 motes for the sender S, receiver R and jammer J. Each mote had a 433 MHz ChipCon CC1000 RF transceiver and used TinyOS 1.1.16 as the operating system. To build the jammer J, we disabled the back off operations to bypass the MAC protocol. Rather than employ a constantly transmitting jammer (which would be easily detectable), we instead employed the *reactive jammer* from [4], where J listens to the channel and, upon detection

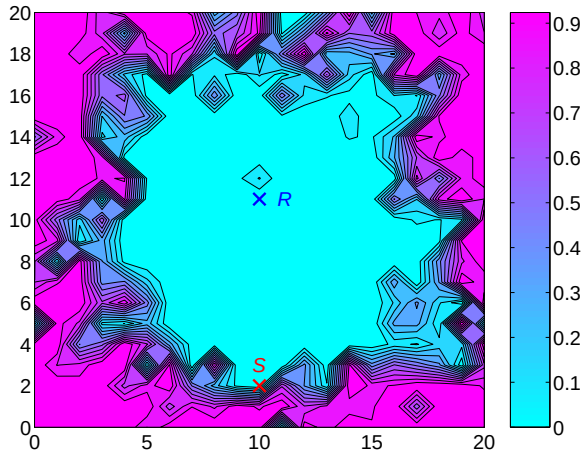


Fig. 4. PDR map vs the jammer's location.

of a preamble, it immediately blasts on the channel by sending a random 2-byte jammer packet.

B. Metrics

We used Packet Delivery Ratio (PDR) to measure the effectiveness of the jamming attack, and consequently to describe the quality of a link should the source increase its power. We measured the PDR at the receiver R by calculating the ratio of the number of packets that pass the CRC check with respect to the total number of sent packets. The total number of sent packets can be obtained through tracking the sequence number of each packet. If no packets are received, the PDR is defined to be 0.

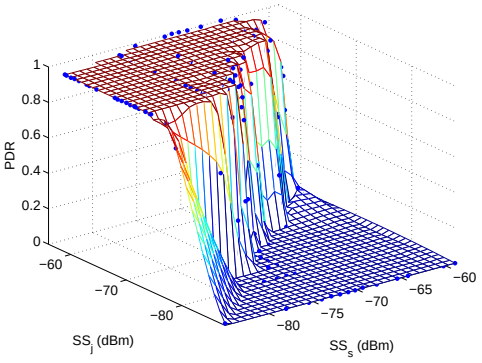
C. PDR vs. Different Jammer Locations

The interference level caused by a jammer to a wireless node is governed by both its transmission power and its location relative to the source and receiver. The closer the jammer is to a node, or the higher transmit power it employs, the greater the impact it will have on network operations. We first study the PDR degradation caused by placing a jammer, with fixed transmit power level, at different locations.

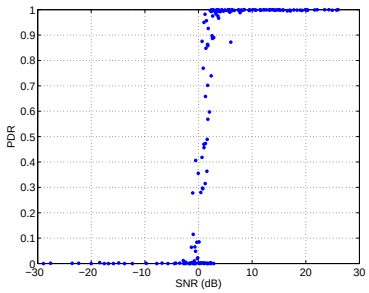
We measured the PDR between S and R over a 20x20 sq. ft. grid. We fixed S at $(10, 2)$, R at $(10, 11)$, and varied J's location from 439 different choices, which are each separated by one foot on the grid. At each location, we measure the PDR from S to R. We set the transmission power of both S and J to their minimum value, $-20dBm$.

Before we present out experiment results, let us first examine the shape of the PDR contour in the ideal case. In a free space, where signal attenuation is purely caused by path loss, the received power is proportional to the distance between the receiver and the sender. In this case, it is the distance between the receiver and the jammer (instead of the location of the jammer) that affects the PDR from S to R. Thus, the contour of the PDR between S and R is a circle centered at the receiver R, and the radius of the contour line that corresponds to zero PDR is determined by the relative transmission power between the sender and the jammer.

In our experiments, we varied the location of the jammer, and measured the corresponding PDR at the receiver. The



(a) Packet delivery rate map VS. power



(b) Packet delivery rate map vs. SNR

Fig. 5. Packet delivery rate map VS. power .

resulting PDR map is shown in Figure 4. Due to the radio irregularity in an indoor environment, the PDR contour is also irregular. We observe that when the jammer is located right next to the receiver, i.e. (10, 12) which is marked by the diamond-shape symbol on Figure 4, the measured PDR value is actually greater than zero. We believe this is caused by the near field effect. Additionally, we observe that the center of the contour line does not coincide with the position of the receiver R, but is biased towards the sender S. This skewness is caused by the nature of the reactive jammer. The efficacy of the reactive jammer is determined by two factors: the ability to detect the preamble of the sender's packets, and the ratio of the sender's power to the jammer's at the receiver side. When the reactive jammer is placed further away from S, it cannot correctly detect the preambles sent by S, and as a result, the packets will not be corrupted, leading to a higher PDR.

D. The Impact of Transmission Power

After studying the impact of the jammer's location, we next looked at the impact of the jammer's transmission power on the PDR at the receiver side. In this set of experiments, we fixed the positions of all three parties, but varied their transmission power settings. Specifically, we placed S, R, and J at (10,2) (10,11), and (7,4) respectively. We gradually increased the transmission power levels of both the jammer (P_j) and the sender (P_s) from $-20dBm$ to $10dBm$, which led to receive levels ranging from $-80dBm$ to $-55dBm$. For a given tuple (P_j, P_s), we measured the PDR over 2000 packet trials, and plot the result in Figure 5.

Figure 5 (a) demonstrates a sharp cliff phenomenon: for any jamming power, as we gradually increase the sender's transmission power above a threshold, the PDR will go

back to 100%. This observation differs from the conclusion conveyed in the theoretical capacity plot(Figure 2), which suggests that for any jamming power, the capacity increases continuously as a function of the sender's transmission power. This is due to framing and packeting.

In Figure 4 (b), we plot the PDR measurements as a function of $\gamma_{S/J}$, the ratio of the received signal power over the jamming power. In this figure, we observe the cliff phenomenon as well, in which PDR goes back to 100% approximately at $\gamma_0 = 2dB$. The cliff phenomenon coincides with the theoretical result, i.e. the success reception of a packet is primarily determined by signal to noise ratio at the receiver. We note that in our experiment, we did not subtract the ambient noise level from the received signal and jamming signal measurement. However, in our case, the abient noise power is much smaller than the signal and jamming power, SNR is approximately $\gamma_{S/J}$.

Our results show that by increasing the transmission power, the sender's transmissions can overshadow the jammer's, and thus successfully reach the receiver. The effectiveness of this strategy is however, largely dependent on the jammer model. For instance, if the jammer operates under a transmission power much higher than what the sender can reach, or if the jammer also dynamically increases its transmission power based on the sender's transmission power (which can be easily achieved by a reactive jammer), then the sender cannot protect the transmissions by raising transmit power. Since the scope of this paper is to study the efficacy of power control in coping with jamming as well as its impact on the overall network performance, we assume the jammer works on a fixed transmission power which is lower than the maximum transmission power a normal node can have.

IV. Jamming and Power Control in Multi-hop scenario

Though our study of the two-node network scenario reveals important insights associated with adapting the transmit power to cope with jamming, a study of the more general multihop network scenario carries more practical significance. In particular, the multihop network scenario, which corresponds to ad hoc and sensor network deployments, inherently involves more complicated interaction between network participants. In this subsection, we thus extend our study to a more general sensor network that consists of multiple nodes. Each node may have one or more neighbors, and each node form links to their neighbor depending on the distance to their neighbors, their transmission power and the abient noise around. We will show that a dynamical power control protocol is necessary to adapt to the network topology.

A. Case Study

In this subsection, we will examine an example network, which consists of five nodes {A, B, C, D, E} with the links depicted in Figure 6 (a). In particular, we will apply the non-isotropic model for jamming to a multihop network. Without loss of generality, we assume that success reception of a packet requires that $SNR > 0dB$, and the transmission power and jamming power are the same. Thus, the jamming

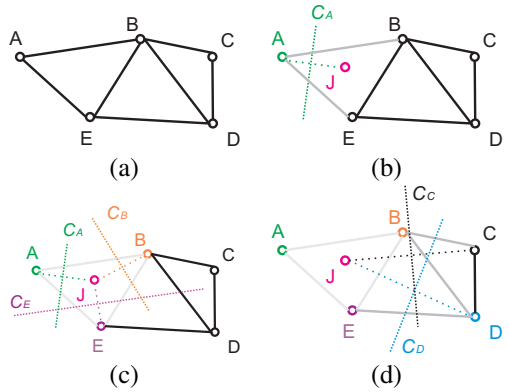


Fig. 6. Multi-node networks topologies: (a) no jammer scenario, (b)-(d) the network topologies affected by the jammer J. (b) Links severed due to the impact the jammer has on A, C_A is the $0dB$ S/J contour line when A is the only sender.(c) Links severed due to the impact the jammer has on B and E, C_B and C_E are the $0dB$ S/J contour line when B or E is the only sender respectively. (d) Links severed due to the impact the jammer has on C and D , C_C and C_D are the $0dB$ S/J contour line when C or D is the only sender respectively.

contour that demarcates the regions within which the node can or cannot receive packets is the bisector of the line segment between the sender and the jammer, as discussed in section II-B. Based on the non-isotropic model, we first show that a jammer will have different impact on links depending on the physical location of the two end nodes of the link. Then we illustrate the power adjustment that individual node should perform to counteract jamming interference.

When a jammer J starts to interfere with legitimate network communications, it will effect links directionally depending on the relative location of the two end nodes that form the link. Take node A as the sender, then the contour C_A splits the jammed region and non-jammed region as a result of jammer J, as shown in Figure 6 (b). All the nodes that located left to C_A will be able to receive packets from A, while all nodes which are located in the fight half plane of C_A cannot receive packets from A. Thus, the links from A to B, L_{AB}, and from A to E, L_{AE}, are severed due to jammer J. Similarly, take B and E as the sender, the links $\{L_{BE}, L_{BA}, L_{EA}, L_{AE}\}$ are jammed by J, as shown in Figure 6 (c). However, the link $\{L_{BC}, L_{BD}, L_{ED}\}$ are not effected. Furthermore, take C and D as the sender, $\{L_{CB}, L_{DB}, L_{DE}\}$ are affected. In summary, the jammer J can have three types of impact on the network: (a) the jammer might kill the link from both direction, e.g. neither ends of the nodes will be able to receive packets from each other, $\{L_{AB}, L_{BA}\}$; (b) the jammer might turn a bidirectional link into a uni-directional link, e.g. C can still receive packets from B, but B cannot hear from D; (c) neither directions of the link are effected, e.g. L_{CD}.

To cope with jamming attacks, the legitimate senders should raise there transmission power so that the jamming region determined by the jammer and the sender will exclude all its neighbors. Therefore, all the potential receivers can successfully decode the messages. As as an example, to compete with jammer J, node A raises its transmission power, which in turn will change the shape and size of the jamming contour. Once the transmission power of the node A is large enough where resulting jamming range divided by the contour C_A doesn't contain all its neighbors, node A can

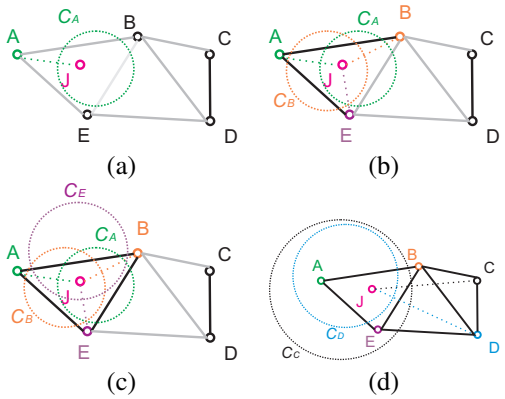


Fig. 7. Using power adjustment to repair the Multi-node networks topologies: (a) the new contour as the result of raising the P_{AT}, (b) the new contour due to increment of P_{BT},(c) increase P_{ET} (d) increase P_{CT} and P_{DT}

resume its ability to send packets to the node B and the node E, as shown in Figure 7 (a). Similar, we illustrated the desire contours that will counteract the jamming impact in Figure 7 (c)-(d).

We note that different sizes of the contours shown in Figure 7 represent different level of transmission power. An accurate calculation on the optimum power setting requires the knowledge on the position of the receivers and the jammer, the jamming power. As those information is not easily available to individual nodes, it is desirable to have a distributed power control protocol which relies on feedback to adjust sender's transmission power.

V. Related Work

Coping with jamming and interference is usually a topic that is addressed through conventional PHY-layer communication techniques. In these systems, spreading techniques are commonly used to provide resilience to interference [5], [6]. Although such PHY-layer techniques can address the challenges of an RF interferer, they require more advanced transceivers and consequently have not found widespread deployment in commercial sensor networks. Instead, most sensor platforms use simpler radios with carrier sensing. Consequently, any form of radio interference that sufficiently elevates the energy in a channel can prevent a sensor from accessing the channel, effectively disrupting communications. We note, though, that the PHY in platforms like the MicaZ or 802.11 do employ a minimal amount of spreading in order to have multipath resistance.

The issue of jamming detection for sensor networks was studied by Wood and Stankovic in [7]. This study employed a measure of the channel's utility to detect jamming, and primarily focused on the issue of mapping the jammed region. The problem of jamming detection was further studied by Xu et al. in [4], where the authors presented several jamming models and explored the need for more advanced form of detection algorithms to identify jamming. Additional jamming strategies were studied by Law et al. [8], and the efficiency of these methods was quantified in terms of the amount of resources needed to conduct an attack. Further work on jamming has studied MAC-layer jamming attacks on reservation-based medium access control schems [9].

Countermeasures for coping with jammed regions in wireless networks has been studied in [1], [10]. In [10], the use of error correcting codes is proposed to cope with jamming. In [1], two countermeasures are presented for coping with jamming. The first method, channel surfing, serves as the motivation for this paper. The second method, spatial retreats, was studied in more detail in [2] and involves mobile sensor nodes physically moving away from the interference source to reestablish connections.

VI. Concluding Remarks

Due to the shared nature of the wireless medium, wireless networks are susceptible to accidental or intentional radio interference. It is therefore important to ensure the wireless communication in the presence of radio interference. To cope with this threat, we have proposed to let the radios compete with the jammer, whereby the network nodes adjust their transmission power to improve the chance for successful communication. In this paper, we have examined the issues associated with using power control both theoretically and experimentally. We begin by exploring the underlying communication theory associated with jamming. We note that the effect of the jammer upon source-receiver communications is not isotropic. We then discuss the potential for improving communication reliability through experiments conducted using Mica2 motes, and in particular explore the feasibility of power-control for competing against jammers. Next, we turn to examining the more complicated scenario consisting of a multi-hop wireless network. We show the complex jamming effect by applying the non-isotropic model of jamming to a multi-hop wireless network, and it is necessary to have a feed-back based power control protocol to compete with jamming interference.

References

[1] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service," in *Proceedings of the 2004 ACM workshop on Wireless security*, 2004, pp. 80 – 89.

[2] K. Ma, Y. Zhang, and W. Trappe, "Mobile network management and robust spatial retreats via network dynamics," in *Proceedings of the The 1st International Workshop on Resource Provisioning and Management in Sensor Networks (RPMSN05)*, 2005.

[3] W. Xu, W. Trappe, and Y. Zhang, "Channel surfing: defending wireless sensor networks from interference," in *IPSN '07: Proceedings of the 6th international conference on Information processing in sensor networks*. New York, NY, USA: ACM Press, 2007, pp. 499–508.

[4] 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*, 2005, pp. 46–57.

[5] J. G. Proakis, *Digital Communications*, 4th ed. McGraw-Hill, 2000.

[6] C. Schleher, *Electronic Warfare in the Information Age*. MArtech House, 1999.

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

[8] Y. Law, P. Hartel, J. den Hartog, and P. Havinga, "Link-layer jamming attacks on S-MAC," in *Proceedings of the 2nd European Workshop on Wireless Sensor Networks (EWSN 2005)*, 2005, pp. 217 – 225.

[9] A. Rajeswaran and R. Negi, "Dos analysis of reservation based mac protocols," in *Proceedings of the IEEE International Conference on Communications*, 2005.

[10] G. Noubir and G. Lin, "Low-power DoS attacks in data wireless lans and countermeasures," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 7, no. 3, pp. 29–30, 2003.