

Jamming Mitigation in Multi-Radio Wireless Networks: Reactive or Proactive?

Sherif Khattab
Computer Science
Department
University of Pittsburgh
Pittsburgh, PA 15260
skhattab@cs.pitt.edu

Daniel Mosse'
Computer Science
Department
University of Pittsburgh
Pittsburgh, PA 15260
mosse@cs.pitt.edu

Rami Melhem
Computer Science
Department
University of Pittsburgh
Pittsburgh, PA 15260
melhem@cs.pitt.edu

ABSTRACT

Jamming is a serious security problem in wireless networks. Recently, software-based channel hopping has received attention as a jamming countermeasure. In particular, proactive, or periodic, channel hopping has been studied more extensively than reactive hopping. In this paper, we address the question of *which of the two defense strategies, namely proactive and reactive channel-hopping, provides better jamming resiliency than the other?* in the context of single- and multi-radio wireless devices. In the single-radio context, we develop theoretical models to analyze the blocking probability for combinations of defense and attack strategies. In the multi-radio setting, we formulate the jamming problem as a max-min game and show through simulation that the game outcome depends on the payoff function. Our results show that reactive defense provides better jamming tolerance than proactive when considering communication availability. However, both reactive and proactive defenses have almost the same performance when energy efficiency is considered as a performance metric.

Categories and Subject Descriptors

C.2.0 [Computer-Communication Networks]: Security and protection (e.g., firewalls)

General Terms

Security, Reliability

Keywords

Jamming, Multi-radio, Max-min Games

1. INTRODUCTION

Wireless jamming aims at blocking wireless communication by keeping the medium busy or by corrupting received signal using radio interference [1]. Channel hopping, whereby radios switch channels to escape jamming, has been proposed to mitigate jamming in wireless sensor networks and 802.11 networks [2, 3, 4, 5]. So far, proactive (periodic) channel-hopping has received more attention than reactive hopping,

whereby in the latter, channel switching occurs only when jamming is detected on the currently used channel.

Proactive channel-hopping has a simpler implementation compared to reactive channel-hopping, which is complicated by the difficulty of jamming detection [6, 3, 4, 5]. However, these issues are closely related to the wireless technology and may be affected by new generations of wireless networks. One of the emerging wireless network paradigms is the multi-radio networks, which have been proposed to increase overall network capacity by exploiting channel diversity [7]. In multi-radio wireless networks, nodes are equipped with multiple radio interfaces operating at orthogonal channels.

In this paper, we address the question of *which defense strategy (reactive or proactive) achieves the best jamming resiliency?* in both single- and multi-radio networks. We decompose this question into two subquestions: (1) *under a given system and attack scenario which of the two defense strategies provides better jamming resiliency?* and, because the attack strategy may be unknown, (2) *which attack strategy is more reasonable for attackers to choose?*

We answer the first subquestion analytically for the single radio case and through simulation for the multiple radio case due to intractability of theoretical analysis in the multi-radio setting. More specifically, we study two attack strategies, namely *scanning* and *sweeping*, whereby scanning jammers have and use the capability of sensing channel activity, whereas sweeping attackers lack (or do not use) this capability and resort to jamming each channel for a fixed amount of time before moving on to other channels. We also consider the effect of the system parameters, such as the number of radios per node, the number of channels, and the delay of jamming detection.

To address the second subquestion, we model jamming as a max-min game between defense and attack. Specifically, we define two games that differ in the optimization metric, or the payoff function. The *availability* game considers communication availability, whereby the defense aims at maximizing availability, and the jamming attack aims at minimizing it. In the *efficiency* game, energy efficiency is considered by both defense and attack. The availability game is relevant in scenarios where data delivery is more important than network lifetime, such as in short-lived emergency-alarm networks. The efficiency game, on the other hand, can be used to model scenarios where extended network lifetime has higher priority, and attackers also want to save energy to extend their jamming lifetime. We study the outcomes

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

SecureComm 2008, September 22 - 25, 2008, Istanbul, Turkey.
Copyright 2008 ACM 978-1-60558-241-2...\$5.00.

of the two games through simulation.

Our main results can be summarized as follows:

- In single-radio networks, reactive defense is provably better than proactive against fast-switching sweeping attack. Against other attacks, formulas are derived to decide which defense strategy is better under different system and attack scenarios.
- In multi-radio networks, reactive defense achieves better jamming tolerance under the availability game. Under the efficiency game, however, both strategies perform almost the same. Therefore, it can be concluded that reactive hopping is a more effective strategy against jamming in multi-radio networks.

The rest of the paper is organized as follows. In the next section we discuss work closely related to the jamming problem. §3 presents the system, defense, and attack models. We present our theoretical analysis of jamming defense and attack strategies in single-radio networks in §4. Our simulation study of jamming in multi-radio networks is described in §5. In §6, we formulate the availability game and analyze its outcome through simulation. §7 introduces energy as a performance metric, defines the efficiency game, and studies it using simulation. We conclude in §8.

2. RADIO JAMMING

Radio jamming is a DoS attack targeting physical and link layers of wireless networks [8, 6]. Radio jamming aims at preventing victim nodes from accessing the shared wireless medium by keeping the medium busy or from successful reception by causing high radio interference at the receiver. Many anti-jamming techniques have been proposed, spanning many layers in the network stack. However, all previous work studies jamming in the context of single-radio networks. This work investigates jamming mitigation in the multi-radio context as well, whereby multiple radios cooperate to deliver data and multiple jammers conspire to cause maximum damage.

Physical-layer defenses: Physical-layer anti-jamming techniques, such as directional (sectored) antennas [9] and spread-spectrum [10], create hard-to-jam “wormholes” within the shared wireless medium [13, 12, 11]. Sectored antennas are potentially effective but not widely deployed. Nodes equipped with spread-spectrum radios [14, 16, 15] are still vulnerable to jamming from nodes with similar radios [3]. Moreover, the recent 802.11a and g standards have replaced frequency hopping, which tolerates jamming but has low bandwidth, with high-bandwidth channel coding schemes, which are vulnerable to jamming [4].

Link-layer defenses: At the link layer, channel hopping improves jamming resiliency in both 802.11 [5, 4] and sensor networks [2, 3]. In channel hopping, channel switching is controlled at the software-level. Channel hopping utilizes the fact that there is a number of orthogonal radio channels in many of today’s wireless standards. The 802.11a standard has been reported to have 12 orthogonal channels [4], 802.15.4 (e.g., CC2420 radio in MICAz motes) has 16 channels [3], and even the older CC1000 radio in Mica2 motes has been reported to allow up to 32 orthogonal channels in the 900MHz band [2]. Two variations of channel hopping have been proposed: proactive and reactive. Augmented

with packet fragmentation and redundant encoding, proactive channel-hopping defends against a wide spectrum of jamming strategies [3]. Proactive channel hopping is coordinated synchronously [5, 4, 3] (assuming loose clock synchronization) and asynchronously for low-bandwidth message delivery [13]. Reactive channel-hopping, or channel surfing, occurs after radio jamming is detected and causes the entire network or only the jammed region to switch to a different radio channel [2].

TDMA-based protocols and multi-frequency link-layer protocols, both static [20] and dynamic [18], mitigate low-power, selective jamming as long as the TDMA and frequency-switching schedules are secure. To mitigate schedule compromise, data blurring with schedule switching [21] and data exfiltration (by time-multiplexing redundant data over multiple channels) [22] have been proposed.

Network-layer defenses: The Jammed Area Mapping (JAM) scheme identifies regions of jammed sensors to be avoided by routing protocols. Jammed sensors “sleep” to outlast jammers [23]. However, intelligent jammers can detect the communication silence and adjust their power consumption accordingly. In spatial retreats, jammed mobile nodes change their physical locations away from jammed areas [24]. This work differs in that the goal is to allow jammed nodes to communicate *while* the jamming attack is on.

3. DEFENSE AND ATTACK STRATEGIES

In this section, we present system and attack models as well as the defense and attack strategies considered in this paper.

3.1 System Model

We consider a multi-radio wireless sensor network, whereby sensors have multiple radios each. The radios of each sensor send redundant data to the base-station over a single hop. Communication is blocked only when *all* radios are jammed at the same time. The *blocking probability* is the fraction of time during which *all* radios are jammed. We also assume that there is a number n_h of orthogonal channels. The base-station has as many wireless transceivers as the orthogonal channels, eliminating the need for simultaneous jamming detection at both sensors and the base-station. Medium access is scheduled between sensors using TDMA. For simplicity of presentation, in what follows only one sensor is considered.

Radios hop among channels, and channel hopping takes a delay of τ time units, which is in the range of tens of microseconds ($80\mu s$ in [18]). A communication radio cannot send or receive data while switching channels. Similarly, a jamming radio cannot jam while switching channels.

3.2 Defense Strategies

We consider two defense strategies: reactive and proactive. The defense strategies differ based on the jamming detection capabilities in the wireless nodes.

Reactive channel-hopping. In the reactive strategy, each radio stays at its current channel as long as no jamming is detected. Once it detects jamming, it switches to a different channel selected uniformly at random. The following detection algorithm is used: If the waiting-time for channel access or for a successful transmission exceeds a threshold, $\delta_d\tau$ (for simplicity of analysis, the threshold is assumed to be a multiple of the channel-hopping delay, τ), jamming is assumed. Only the sensor has to detect jamming and decide

to switch channels; the base-station is already listening on all the channels.

Proactive channel-hopping. In the proactive defense strategy, all radios of a sensor switch channels periodically. That is, every $s_d\tau$ time units, they switch channels, and they reside at their channels for $(s_d - 1)\tau$ time units. The proactive strategy is oblivious to jamming status, so unjammed radios may be triggered to switch and jammed ones may be kept at their channels. Clock synchronization between the sensor and the base-station is not needed because the base-station has enough transceivers to cover all channels.

3.3 Attack Model and Strategies

The jamming attack is launched by a number of attack radios, whereby each attack radio can jam one channel at a time. For instance, a compromised sensor can jam communication by overriding the MAC-protocol and sending packets continuously (low-power attack methods are also feasible [6]). We assume that Spread Spectrum (SS) [10] by itself cannot prevent this jamming attack, as the jammers may use the same SS hardware as the attacked radios. We also assume that if a channel is jammed, no data can be communicated at that channel.

We consider two attack strategies, namely **scanning** and **sweeping**; both have been proposed elsewhere [3, 4, 5]. In both strategies, attackers hop channels such that the jammed channels change over time. The two attack strategies differ in the *activity-sensing* capability of attackers as follows.

Scanning attack. Scanning attackers sense legitimate channel activity to determine if the channel they jam is being used or not. Each attack radio keeps hopping until it finds a channel that has legitimate activity, and it stays there until it detects lack of activity. It takes an attack radio a *channel-sensing time*, $\delta_x\tau$, to determine channel activity or lack thereof. This delay depends on the legitimate traffic rate and on how frequently the attack radio stops jamming to sense the medium activity. After this delay, the attack radio selects its next channel uniformly at random.

It should be noted that the attack radio has two possibilities in selecting the next channel: from all channels and from channels not previously visited since last encounter with an active channel. The second option is more effective if the communication radio would stay put at its channel until being “caught” by the jammer. This is guaranteed to happen only if the defense strategy is reactive and there is only one jamming radio. In the analysis in §4, whereby there is one jamming radio and the defense strategy is assumed to be known, we assume that attackers use the second option; the first option is assumed otherwise.

Sweeping attack. Sweeping attackers periodically and simultaneously switch channels irrespective of channel activity, and they jam their channels until the next period. In other words, each sweeping radio changes the jammed channel every $s_x\tau$ time units and jams the channel for $(s_x - 1)\tau$ time units. It selects the next channel uniformly at random. Two variations are considered: *fast-sweeping*, where attackers switch every τ (the channel-hopping delay), and *slow-sweeping*, where the period length is a multiple of τ .

In both attack strategies, attack radios coordinate so that no two radios jam the same channel at the same time in order to cause the maximum damage.

4. CHANNEL-HOPPING IN SINGLE-RADIO NETWORKS

In this section, we compare proactive channel-hopping against reactive channel-hopping in single-radio networks under the scanning and sweeping attack strategies with the goal of answering the question of *under a given system and attack scenario which defense strategy provides better jamming resiliency?* In what follows, it is assumed for ease of presentation that time variables are measured in units of τ , the channel-hopping delay.

4.1 Sweeping Attack

First, the blocking probability (defined in §3.1) is studied against the sweeping attack.

LEMMA 1. *In single-radio networks, the blocking probability of reactive channel-hopping against sweeping attack is*

$$P_b^{\text{reactive-sweeping}} = \begin{cases} \frac{1+\delta_d}{n_h s_x} & \text{when } (s_x - 1) \geq \delta_d; \\ \frac{s_x - 1}{n_h s_x} & \text{otherwise.} \end{cases}$$

where δ_d is the jamming detection delay, n_h the number of channels, and s_x the period of the sweeping jammer.

PROOF. Every period, the sweeping attacker selects a channel uniformly at random, and thus, it hits the channel used by the communication radio with a probability $\frac{1}{n_h}$, where n_h is the total number of channels. Consider two cases.

(1) $(s_x - 1) \geq \delta_d$: The radio detects jamming and hops to another channel. Therefore, the radio stays blocked for $\delta_d + 1$ if hit by the jammer, where δ_d is the time it takes the radio to detect jamming and 1 is the channel-hopping delay during which the radio cannot communicate as well. Hence, the expected blockage time in each attack period is $\frac{1+\delta_d}{n_h}$, resulting in a blocking probability of $\frac{1+\delta_d}{n_h s_x}$.

(2) $(s_x - 1) < \delta_d$: The radio cannot detect that it is being jammed and will stay blocked for the whole attack residence time, $s_x - 1$, if hit by the jammer, resulting in a blocking probability of $\frac{s_x - 1}{n_h s_x}$. \square

The blocking probability of **proactive defense against sweeping attack** is then derived. To give an intuition, consider the following example: Assume that the defense period is 3 time units, the attack period is 2 time units, and thus, the least common multiple (hyperperiod) of the two periods $LCM = 6$ time units. Note that in this example the radio is readily blocked for $2 = \frac{LCM}{3}$ time units, during which it is hopping channels. Also, the radio is free for $2 = \frac{6}{2} - 1$ time units due to the attacker hopping channels and consequently not jamming (the attacker hops in 3 time units but in one of them the radio is blocked because it is hopping channels itself). In the remaining 2 time units (out of the 6 time units of the hyperperiod length), both the radio and the jammer are not hopping and are residing on some channel. Again, because both defense and attack radios select channels uniformly at random, the probability that both the radio and the jammer reside on the same channel is $\frac{1}{n_h}$, and thus, the radio is blocked for $\frac{2}{n_h}$ time units on average. So, there are $2 + \frac{2}{n_h}$ blocked time units on average out of the $LCM = 6$ time units, resulting in a blocking probability of $\frac{2 + \frac{2}{n_h}}{6}$.

LEMMA 2. *In single-radio networks, the blocking probability of proactive channel-hopping against sweeping attack*

is

$$\frac{1}{s_d} + \frac{1 - \frac{1}{s_d} - \frac{1}{s_x}}{n_h} \leq P_b^{\text{proactive-sweeping}} \leq \frac{1}{s_d} + \frac{1 - \frac{1}{s_d} - \frac{1}{s_x} + \frac{1}{LCM}}{n_h}$$

where s_d is the channel-hopping period of the proactive defense, s_x the period of the sweeping jammer, and LCM the least common multiple of s_d and s_x , or the hyperperiod.

PROOF. Let LCM be the hyperperiod length, that is, the least common multiple of defense and attack periods. Let $LCM = ps_d = qs_x$, for some integers $p > 0$ and $q > 0$. During any hyperperiod, there are p time units when the communication radio is hopping and q time units when the attacker is hopping. Depending on the defense and attack periods and their phase shift, there exist time slots when both attack and defense radios hop channels simultaneously or the defense and attack hopping instances never intersect.

Consider first the case that there is intersection between attack and defense hopping instances. Without loss of generality, consider the hyperperiod that ends at one of the intersections. By definition of the hyperperiod, exactly one of the q attack hopping instances (specifically, the last hopping instance in the hyperperiod) coincides with a hopping instance of the communication radio. Therefore, out of the LCM time units of the hyperperiod, the radio is hopping in p and the jammer is hopping for q time units, but both are hopping together for one time unit. Hence, both the communication radio and the attacker are not hopping and are residing on some channel for $(LCM - p - q + 1)$ time units.

The radio is blocked in the p hoppings. It is also blocked for $\frac{1}{n_h} \cdot (LCM - p - q + 1)$ time units on average, where again $\frac{1}{n_h}$ is the probability that the jammer hits the channel used by the radio. Hence, the expected number of blocked time units during each hyperperiod is $(p + \frac{LCM - p - q + 1}{n_h})$, resulting in a blocking probability of $\frac{p + \frac{LCM - p - q + 1}{n_h}}{LCM}$.

Now, consider the case that the hopping instances of the defense and attack never intersect. There are still p blocked time units in which the radio is hopping channels. However, the number of time slots during which the radio and the jammer are not hopping is $(LCM - p - q)$ time units, one less than in the previous case, because there is no intersection between attack and defense hopping instances. This results in an expected number of blocked time units of $(p + \frac{LCM - p - q}{n_h})$ during each of the hyperperiods, and the blocking probability is $\frac{p + \frac{LCM - p - q}{n_h}}{LCM}$. \square

The proof of the next theorem follows directly from comparing the blocking probabilities in Lemma 1 and Lemma 2.

THEOREM 1. *Against sweeping attack in single-radio networks, (a) when $\delta_d > s_x - 1$, reactive channel-hopping achieves less or the same blocking probability as proactive channel-hopping and (b) when $\delta_d \leq s_x - 1$, reactive channel-hopping achieves less blocking probability if $\delta_d < s_x - 1 + ((n_h - 1)\frac{s_x}{s_d} - 1)$ and proactive channel-hopping achieves less blocking probability if $\delta_d > s_x - 1 - (1 - \frac{s_x}{LCM} - (n_h - 1)\frac{s_x}{s_d})$.*

Theorem 1 supports the intuition that the best defense against a jammer that sweeps the channels very fast ($(s_x - 1) < \delta_d$) is to stay put. Indeed, the stay-put radio can be viewed as a reactive radio with jamming detection delay (δ_d) longer than attack residence-time ($s_x - 1$) (the reactive radio would not detect jamming and would not switch channels). Part (a) of the theorem states that the reactive radio achieves less or the same performance as the proactive radio⁹.

Against a slow sweeping attacker, reactive channel-hopping is better than proactive as long as the radio has some jamming-free time after it detects jamming and moves to a different channel. The next corollary formalizes this condition.

COROLLARY 1. *Against sweeping attack in single-radio networks, reactive channel-hopping achieves less blocking probability than proactive if $\delta_d \leq s_x - 1$ and $(s_x - 1) - \delta_d > 1$.*

The corollary follows from part (b) in Theorem 1, where reactive achieves less blocking probability when $\delta_d < s_x - 1 + ((n - 1)\frac{s_x}{s_d} - 1)$, or $(s_x - 1) - \delta_d > (1 - (n - 1)\frac{s_x}{s_d})$. Noting that $(n - 1)\frac{s_x}{s_d} \geq 0$, the condition is true if $(s_x - 1) - \delta_d > 1$. The following example illustrates the above corollary. If $s_x = 10$ time units, $\delta_d = 7$ time units (as in 802.11 retransmission threshold), and $n_h = 12$ channels (as in 802.11a), the blocking probability of the reactive defense will be $\frac{1+7}{12-10}$ (the first case in Lemma 1), and there is no value of s_d that makes proactive defense achieves less blocking probability; even when $s_d = \infty$, the minimum blocking probability of the proactive defense is $\frac{9}{12-10}$ (the lower bound in Lemma 2). However, if $s_x = 8$, the blocking probability of the reactive defense becomes $\frac{1+7}{12-8} = \frac{1}{2}$, and the proactive defense achieves less blocking probability for $s_d > 88$.

4.2 Scanning Attack

The blocking probability under the scanning attack is now considered. In what follows, for simplicity, time is assumed to be slotted, and the slot time is assumed to be equal to the time it takes the attacker to detect lack of channel activity and hop. That is, the slot time is $\delta_x + 1$. Let α denote the ratio between the channel-hopping delay and the slot time, that is, $\alpha = \frac{1}{\delta_x + 1}$. For simplicity, it is also assumed that the time it takes the radio to detect jamming and hop channels, that is, $\delta_d + 1$, is a multiple of the time slot length [4].

Expressions for the blocking probability of the **reactive defense against the scanning attack** are then derived. To this end, we use the following Markov model: The model has two classes of states: in the B states the radio is blocked (or jammed) and in the F states the radio is free from jamming. State B_i represents that the radio has been jammed for i time slots, and state F_i represents that the jammer is still scanning for the radio and has i channels yet to visit.

Once the radio is in the first B state (B_1), it stays blocked for $(\delta_d + 1)$ time units, which is the time to detect jamming and hop to another channel. This time interval corresponds to $\frac{\delta_d + 1}{\delta_x + 1}$ states, because of our assumption that the time is slotted into $(\delta_x + 1)$ -sized time slots. Also, the transition probability from each state B_i to B_{i+1} is 1 to represent the deterministic jamming-detection and hopping delays.

After the radio hops to a different channel, it stays free from jamming for at least one time slot (state $F_{n_h - 1}$) while the

⁹ Same performance is achieved only when the proactive radio has a period $s_d = \infty$, that is, stay-put.

jammer senses lack of channel activity and hops channels. The jammer selects its next channel uniformly at random from $n_h - 1$ channels. The probability that the jammer hits the channel used by the radio and drives the radio back into the first blocked state is $\frac{1}{n_h - 1}$, which is the transition probability from state $F_{n_h - 1}$ to state B_1 . The transition probability from state $F_{n_h - 1}$ to $F_{n_h - 2}$ is the probability that the jammer misses, which is $1 - \frac{1}{n_h - 1} = \frac{n_h - 2}{n_h - 1}$. Similarly, at state $F_{n_h - i}$, the jammer chooses its next channel out of $n_h - i$ channels, hitting the used channel with probability $\frac{1}{n_h - i}$ and missing with probability $\frac{n_h - i - 1}{n_h - i}$. This process may continue until the jammer scans all the channels but one (state F_1), in which case it hits the channel used by the radio with probability 1 in the next time slot.

LEMMA 3. *In single-radio setting, the blocking probability of reactive channel-hopping against a scanning attack is*

$$P_b^{\text{reactive-scanning}} = \frac{1}{1 + \frac{n_h(\delta_x + 1)}{2(\delta_d + 1)}}$$

PROOF. In the Markov model described above, the transition probabilities yield the following equations: $\pi_{B_1} = \pi_{B_1} \dots = \pi_{B_1} \frac{\delta_d + 1}{\delta_x + 1} = \pi_{F_{n_h - 1}}$, where the π 's are the steady-state probabilities of the Markov model. Also, $\pi_{F_{n_h - 2}} = \frac{n_h - 2}{n_h - 1} \pi_{F_{n_h - 1}}$ and $\pi_{F_{n_h - 3}} = \frac{n_h - 3}{n_h - 2} \pi_{F_{n_h - 2}} = \frac{n_h - 3}{n_h - 2} \cdot \frac{n_h - 2}{n_h - 1} \pi_{F_{n_h - 1}} = \frac{n_h - 3}{n_h - 1} \pi_{F_{n_h - 1}} = \frac{n_h - 3}{n_h - 1} \pi_{B_1}$. In general, $\pi_{F_{n_h - i}} = \frac{n_h - i}{n_h - 1} \pi_{B_1}$. Also, the sum of the steady-state probabilities of all states is 1, that is, $\sum_{j=1}^{\delta_d + 1} \pi_{B_j} + \sum_{i=1}^{n_h - 1} \pi_{F_i} = 1$. Substituting in this equation to solve for π_{B_1} yields: $\frac{\delta_d + 1}{\delta_x + 1} \pi_{B_1} + n_h \pi_{B_1} - \frac{n_h}{2} \pi_{B_1} = 1$. Thus, $\pi_{B_1} = \frac{1}{\frac{\delta_d + 1}{\delta_x + 1} + \frac{n_h}{2}}$. Noting that the blocking probability is the summation of the steady-state probabilities of the B states, that is, $\sum_{j=1}^{\delta_d + 1} \pi_{B_j} = \frac{\delta_d + 1}{\delta_x + 1} \pi_{B_1} = \frac{1}{1 + \frac{n_h}{2\alpha(\delta_d + 1)}}$. \square

LEMMA 4. *In single-radio networks, the blocking probability of proactive channel-hopping against a scanning attack is:*

$$P_b^{\text{proactive-scanning}} = \frac{\frac{2n_h}{\delta_x + 1} + s_d(s_d - 1)}{2n_h(s_d - 1 + \frac{1}{\delta_x + 1})}$$

PROOF. In Eqn. 2 of [4], which uses the same assumptions as in Lemma 3, the throughput of the proactive defense against the scanning attack is derived as $\frac{2n_h(s_d - 1) - s_d(s_d - 1)}{2n_h(s_d - 1 + \alpha)}$, where $\alpha = \frac{1}{\delta_x + 1}$. The throughput is defined as the fraction of time the communication is not jammed. By definition, the blocking probability is 1 minus the throughput, resulting in the formula presented in the lemma. \square

The proof of the next theorem follows directly from comparing the blocking probability in Lemma 3 and Lemma 4.

THEOREM 2. *In single-radio networks, reactive channel-hopping achieves less blocking probability than proactive channel-hopping against scanning attack if and only if*

$$\frac{1}{1 + \frac{n_h(\delta_x + 1)}{2(\delta_d + 1)}} < \frac{\frac{2n_h}{\delta_x + 1} + s_d(s_d - 1)}{2n_h(s_d - 1 + \frac{1}{\delta_x + 1})}$$

For example, when $\delta_x = \delta_d = 1$ and $n_h = 12$ (the number of channels in 802.11a), Theorem 2 reduces to that reactive achieves less blocking probability if and only if $7s_d^2 - 31s_d + 96 > 0$. This quadratic expression is > 0 for all values of s_d , meaning that reactive achieves less blocking probability than proactive for these parameter values. However, the window over which proactive defense achieves better performance increases with slower jamming detection. For instance, with the same example but with $\delta_d = 7$, proactive defense achieves less blocking probability than reactive for $1.9 < s_d < 8.66$ time units. The bounds are the roots of the quadratic equation $5s_d^2 - 53s_d + 84 = 0$.

In summary, reactive channel-hopping achieves better jamming resilience than proactive channel-hopping for most of the spectrum of attack and system parameters against both scanning and sweeping attacks in single-radio networks. The next section studies the relative performance of reactive and proactive strategies in multi-radio networks. As will be shown, the reactive strategy continues to outperform the proactive strategy in multi-radio networks.

5. CHANNEL-HOPPING IN MULTI-RADIO NETWORKS

This section analyzes the jamming problem in multi-radio networks. Due to intractability of theoretical analysis in this case, simulation is used to compare proactive and reactive channel-hopping against the two attack strategies. The goal is also to determine the best defense strategy under a given system and attack scenario.

Table 1: Simulation parameters for comparing reactive and proactive channel-hopping strategies (Bold face represents default values)

Parameter	Values
Number of communication radios	[1-9], 3
Number of attack radios	[3-11], 3
Number of channels	[4-24], 12
Channel-hopping delay	0,1,2,3,4,5
Period for proactive defense	10
Period for sweeping attack	1 (fast), 10 (slow)
Jamming-detection threshold	1,2,3,4,5,6,7,8,9,10
Attacker channel-sensing time	1
communication power	40mW
jamming power	40mW
Channel-hopping power	[0-40], 0mW

To this end, a simulation study was conducted to analyze the interaction between defense and attack strategies in multi-radio networks. Simulation time is divided into slots, where each time slot represents the time to transmit one packet, or what we call the packet-time².

Table 1 summarizes the parameters used. The number of channels was varied from 4 as in the 433MHz band of CC1000 radio up to 24 with a default value of 12 as in 802.11a. The number of communication radios was varied from 1 to 9, and

²Wood *et al.* shows that each packet should be divided into fragments and the fragment time should be in the order of the channel-hopping delay to prevent a fast-switching attacker from disrupting communication on all channels [3]. We use the packet fragment time as the slot time.

the number of communication and attack radios was set to be the same unless otherwise specified.

The packet-time was used as the unit for time-based parameters. The channel-hopping delay was varied from 0 up to 5 packet-time with a default value of 1 packet-time. The period of the proactive hopping strategy was set at 10 (corresponding to 10% hopping cycle). The jamming-detection threshold was set to 7 packet-time (as in 802.11 retransmission threshold) by default and varied in an experiment between 1 and 10 packet-time. The attack channel-sensing time was set to 1 packet-time as a worst-case of a highly effective attacker. The energy-related parameters will be discussed in §7.

Each experiment compares the performance of all combinations of attack (scanning, fast-sweeping, and slow-sweeping) and defense (reactive and proactive) strategies. Each experiment run lasted for about one million packet-time and the average of 10 runs is reported. The 90% confidence intervals were smaller than 2% of the average reported at each data point and are not shown to improve presentation.

In the first set of experiments, the number of communication radios was varied, and the number of attack radios matched the number of communication radios. As shown in Fig. 1, as more radios are used, the blocking probability decreases, except for scanning attack against both proactive and reactive defenses. To explain, recall that both defense and attack radios are increased simultaneously in this experiment and note that when the number of radios exceeds half the total number of channels (a total of 12 channels is used in the simulations), there are always ($2 \times$ number of radios – number of channels) radios that have no room to escape if they get jammed. However, only the scanning attackers can make full usage of this situation; sweeping attackers are limited because they do not sense channel activity and may hop away from an active channel. It can also be observed that the blocking probability for proactive defense is always at least 10%. This is expected due to the hopping cycle of 10%; every 10 packet-time, one packet-time is blocked during channel hopping.

It was observed that with a single radio both proactive and reactive defense strategies performed almost the same against the scanning attack. This observation may explain the use of proactive defense in previous channel-hopping research (e.g., [5,4]); proactive defense is much simpler to implement and achieves the same performance as reactive. As more radios are used, the reactive defense strategy achieved strictly less blocking probability than the proactive strategy against all attack strategies. The simulation results (at number of radios = 1) matched the models presented in the previous section, except for the scanning attack. This difference is intentional and expected. Whereas the model assumes that the scanning attacker keeps history of its visited channels and avoids them when selecting its next channel, in the simulation it is assumed that the attacker selects its next channel without keeping history.

In the second experiment, the total number of channels was varied while fixing the number of radios and attackers at three. Fig. 2 shows that, as expected, with more channels the blocking probability decreased. The reactive strategy achieved better performance than the proactive strategy against all attack types.

Other experiments were conducted where the number of

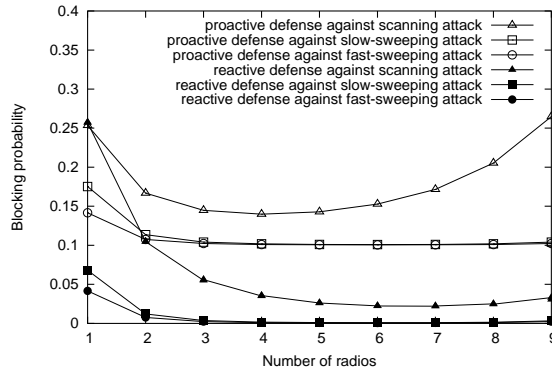


Figure 1: Effect of number of radios of both defense and attack on the communication blocking probability; 12 channels.

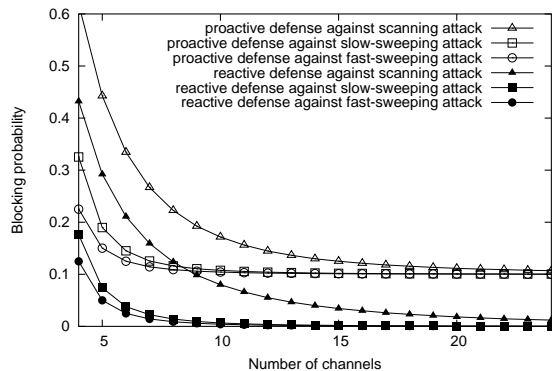


Figure 2: Effect of number of channels on the communication blocking probability; 3 radios.

attack radios (with fixed number of defense radios), the channel-hopping overhead, the jamming-detection threshold, the attack channel-sensing delay, and the period of proactive defense were varied. A similar interaction was observed between defense and attack strategies, that is, reactive channel-hopping achieved less or the same blocking probability compared to proactive channel-hopping.

6. THE DEFENSE-ATTACK AVAILABILITY GAME

The previous discussion addressed the question of which defense strategy is better given an attack strategy. This section addresses the case when the attack strategy is not known. To this end, the jamming defense problem is modeled as a max-min game [25] between defense and attack. Two payoff functions are considered, communication availability (analyzed in this section) and energy efficiency (analyzed in the next section). This section defines the availability game and analyzes its outcome using simulation. We start by a brief background on max-min games.

6.1 Max-min Games

A max-min game (also known as a zero-sum game) [25] involves two players with each player's gain maximized when the gain of the other player is minimum. Each player has a set of actions, and a payoff function is defined over the

action pairs. The payoff of one player can be viewed as the negative of the other's. An example of a payoff function is shown in Table 2. Player 1 has two actions: x_1 and x_2 . Player 2 has three actions: y_1, y_2 , and y_3 . The values shown in the table are those of player 1 (payoff for player 2 is the negative of these values).

The steady state of a max-min game is when each player cannot get a higher payoff by acting unilaterally. The *Nash equilibrium* [25] represents this state. An action pair (x^*, y^*) is a Nash equilibrium if and only if each of the actions x^* and y^* is a *maximizer* [25]. That is,

$$\min_{y \in A_2} u_1(x^*, y) \geq \min_{y \in A_2} u_1(x, y) \text{ for all } x \in A_1, \text{ and}$$

$$\min_{x \in A_1} u_2(x, y^*) \geq \min_{x \in A_1} u_2(x, y) \text{ for all } y \in A_2.$$

where $u_i()$ and A_i are the payoff function and the set of actions for player i .

In other words, a maximizer is an action that maximizes the payoff that the player can guarantee, taking into consideration that the other player wants to cause the maximum damage [25]. The maximizer of player 1 solves the problem $\max_x \min_y u_1(x, y)$. The maximizer of player 2 solves the problem $\max_y \min_x u_2(x, y)$.

In the game in Table 2, the Nash equilibrium is the action pair (x_2, y_1) . Both players cannot get higher payoff by choosing a different action alone. For instance, if player 1 chooses action x_1 instead, he will get a lower payoff (4 instead of 5). Although the example has only one solution, there may be, in general, more than one Nash equilibrium.

6.2 Availability Game

In the availability game, the main goal of the network is to deliver data. The attack on the other hand aims at blocking communication for as much time as possible. The blocking probability, $P_b(d, a, S)$, in this game is the percentage of time communication is blocked, whereby communication is blocked only when *all* radios are jammed. The blocking probability depends on the defense strategy (d), attack strategy (a), and system parameters (S), such as the number of radios and the number of channels. The communication availability is $1.0 - P_b(d, a, S)$.

The *maximizer* defense strategy is the one that guarantees the maximum availability knowing that the attack aims at minimizing it. It solves the problem:

$$\arg \max_{d \in \mathcal{D}} \min_{a \in \mathcal{A}} P_b(d, a, S)$$

where $\mathcal{D} = \{\text{proactive, reactive}\}$ are the defense strategies and $\mathcal{A} = \{\text{scanning, fast-sweeping, slow-sweeping}\}$ are the attack strategies.

To determine the solution of the availability game defined above, that is, to find the maximizer defense strategy, recall that in Fig. 1 the reactive defense achieved better

Table 2: An example payoff function for a max-min game.

	y_1	y_2	y_3
x_1	4	7	2
x_2	5	6	8

performance than proactive except for the single-radio setting, whereby they both achieved almost the same performance. Also, the scanning attack strategy achieved more damage (higher blocking probability) than the sweeping attack (the bottom two curves in Fig. 1) against reactive defense. It can be concluded that the best attack strategy in the availability game is the scanning strategy. This leads to the following observation under the studied system parameters: **The Nash equilibrium in the availability game is $\langle \text{reactive, scanning} \rangle$ in multi-radio networks. In single-radio networks, there are two Nash equilibria $\langle \text{reactive, scanning} \rangle$ and $\langle \text{proactive, scanning} \rangle$.**

7. USING ENERGY EFFICIENCY AS PERFORMANCE METRIC

Through the previous discussion, the focus was on communication availability. However, wireless networks are usually limited in their energy resources, and thus, taking the energy consumption into consideration is crucial to determine the best defense strategies. This section analyzes the jamming problem as an energy-efficiency problem. In this context, the question of which defense strategy is better is first answered. Then, a max-min game is defined with energy efficiency as the payoff function, and its outcome is analyzed using simulation.

7.1 Energy Model

A metric that emphasizes energy efficiency is used. Specifically, the used metric is the Jamming Defense Power Efficiency (JDPE), which represents the communication availability achieved per unit energy, and the energy is defined relative to the attack energy consumption.

$$JDPE(d, a, S) = \frac{1.0 - P_b(d, a, S)}{\frac{\text{defense power consumption}}{\text{attack power consumption}}} \quad (1)$$

In order to define the power consumption of defense and attack in Eqn. 1, an energy model is incorporated into the simulator. A radio is either in stationary or channel-hopping states. While in stationary state, a communication radio tries to send and receive data whereas an attacker jams. Let the average power consumed by a radio while in stationary state be PS_d (PS_a for attack), and the power consumed in channel-hopping state PC_d (PC_a for attack). The average power consumed by the defense is a weighted sum of stationary power and channel-hopping power: $ws_d \cdot PS_d + wm_d \cdot PC_d$, where the weights (ws_d and wm_d) are the average over time of the number of defense radios in the stationary and hopping states, respectively. Similarly, the average attack power is: $ws_a \cdot PS_a + wm_a \cdot PC_a$, where the weights (ws_a and wm_a) are similarly defined.

The attack and defense stationary power was set to 40mW [15]. Equal values of stationary power were selected for both defense and attack based on the feasibility of low-power jamming attacks [21, 17, 3, 6]. The power consumed while hopping was varied from 0mW (i.e., channel hopping consumes negligible power compared to transmit/receive power [14]) to 40mW (similar to stationary power).

7.2 Simulation Results

In the first experiment, the number of radios was varied with a matching number of attackers. When a single radio is used,

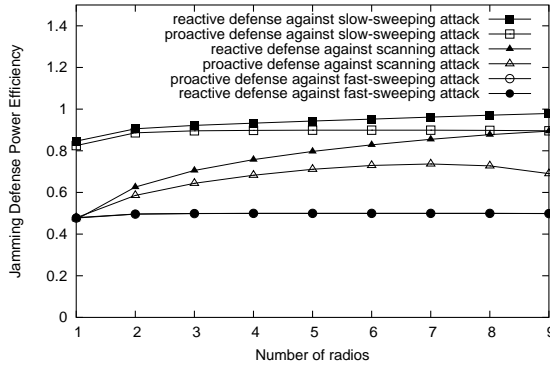


Figure 3: Effect of number of radios on JDPE; 12 channels.

both proactive and reactive strategies performed almost the same (Fig. 3), again explaining the adoption of proactive defense in single-radio networks [5, 4]. With more radios, the JDPE improved except for scanning attack against proactive defense (when number of radios exceeded half the channels). This trend is similar to the proactive-scanning curve in Fig 1, which was explained previously. It was also observed that the reactive strategy performed better (higher JDPE) than proactive except against fast-sweeping attack, where they both achieved exactly the same JDPE (the bottom two lines in Fig. 3). Whereas reactive defense achieved less blocking probability against fast-sweeping attack (Fig. 1), this advantage was neutralized as it also consumed more power because of spending more time in communication.

In the next experiment, the total number of channels was varied while fixing the number of radios (for both defense and attack) at three. As shown in Fig. 4, against the sweeping attack (both slow and fast), the JDPE increased at first and then saturated at six channels for both reactive and proactive strategies. To explain, note that the relative energy consumption of proactive defense vs. fast-sweeping attack is independent of the number of channels; in the fast-sweeping attack, no matter how many channels there are, defenders (attackers) in this combination transmitted (jammed) for 9 (1) packet-time and hopped for 1 packet-time. Noting that the transmission and jamming energy consumption is the same and channel-hopping energy is 0, the proactive defense consumed $\frac{9}{5}$ more energy than fast-sweeping attack. Thus, the saturation of JDPE is mainly

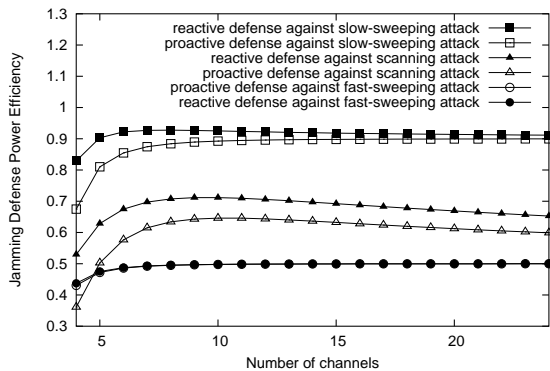


Figure 4: Effect of number of channels on JDPE; 3 radios.

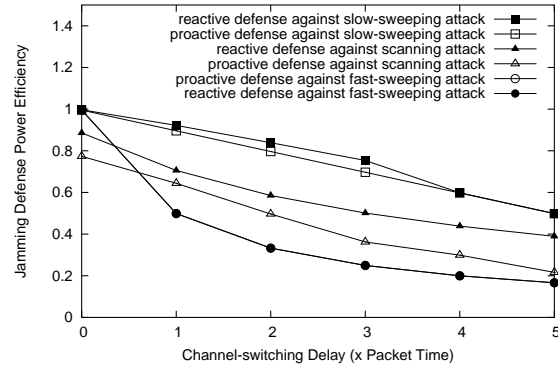


Figure 5: Effect of channel-hopping delay on JDPE. 3 radios and 12 channels.

due to the almost constant blocking probability after 6 channels (in Fig. 2).

The saturation of JDPE in the fast-sweeping vs. reactive case has a different reason. Because the blocking probability kept on decreasing after 6 channels (bottom curve in Fig. 2), radios spent more time transmitting and receiving. Consuming more power, the relative defense-to-power consumption increased resulting in almost constant JDPE (Eqn. 1).

The JDPE in proactive defense vs. slow-sweeping attack followed the trend of the blocking probability in Fig. 2: improving until around 10 channels then staying constant. A slight decrease in JDPE after 6 channels in the reactive vs. slow-sweeping scenario was also observed. This is because radios spent more time unjammed and thus consumed more power in transmission/reception, while the sweeping attackers have constant power consumption.

Against the scanning attack, both reactive and proactive defenses failed to maintain the improvement in JDPE after around 10 channels. With more channels, the radios have more chance to escape, and the scanning attackers hop more often, because a scanning attacker stays one packet-time at an idle channel before it hops to another, whereas it stays eight packet-time at an active channel before the jammed radio detects jamming and hops away. Thus, they spend more time in the zero-power channel-hopping state.

In the next experiment, the channel-hopping delay was varied. As channel-hopping delay increased, the JDPE worsened for all defense-attack combinations as expected (Fig. 5). Reactive defense was more efficient than proactive except against fast-sweeping attack, whereby both achieved the same performance.

As can be observed from Fig. 6, increasing the channel-switching power (PC_d and PC_a in §7.1) resulted in improving JDPE in all defense-attack combinations except for proactive defense against slow-sweeping attack. The fast-sweeping attackers consume half of their time hopping channels, and thus, they suffered the most from increasing the hopping energy cost, resulting in the steepest increase in JDPE. On the other hand, slow-sweeping attackers consume only 10% of their time hopping channels, and thus, are the least impacted by the increasing hopping power. Because the hopping cycle is the same for slow-sweeping

attackers and proactive radios, the JDPE in their combination was not affected by the hopping power. When the channel-switching power reached the communication (jamming) power of 40mW, the effect of energy consumption on JDPE was neutralized, and JDPE was only affected by the blocking probability; the relative order among the defense-attack combinations at $PC_d = PC_a = 40\text{mW}$ is the reverse of their order in Fig. 1 at $n_f = n_x = 3$;

The jamming-detection threshold affected only the reactive defense strategy as expected (Fig. 7). Although it may be expected that faster reaction to jamming would result in better performance for the reactive defense, its JDPE worsened at short jamming-detection thresholds against scanning attack. The blocking probability indeed improved at shorter thresholds. However, radios spent more time unjammed and consequently spent more power in transmission/reception, and attackers spent more time channel-hopping, resulting in a small JDPE. Other than this point in the curve, reactive was more or same energy-efficient as proactive.

In the last experiment, the number of attack radios was varied while fixing the number of defense radios (Fig. 8). Increasing the number of attackers had two effects: increased blocking probability and increased attack power consumption. At first, blocking probability did not increase as fast as the attack power consumption resulting in improving JDPE. However, the blocking probability kept on increasing until its effect took over and resulted in a worsening JDPE. The turning point was different in different defense-attack combinations. In all scenarios, reactive defense achieved better or same performance as proactive defense.

In summary, the reactive hopping strategy achieved the same or higher energy-efficiency than proactive hopping against the three attack strategies except against the scanning attack and only when the jamming-detection threshold is very small.

7.3 Efficiency Game

A max-min game between defense and attack is defined to determine the most “reasonable” attack strategy to deplete network energy, in case the attack strategy is not specified a priori. The efficiency game takes energy consumption of both defense and attack into consideration. In this game, the network aims at delivering as much data as possible while extending its lifetime. Attackers on the other hand aim at incurring as much damage as possible with as low energy as possible.

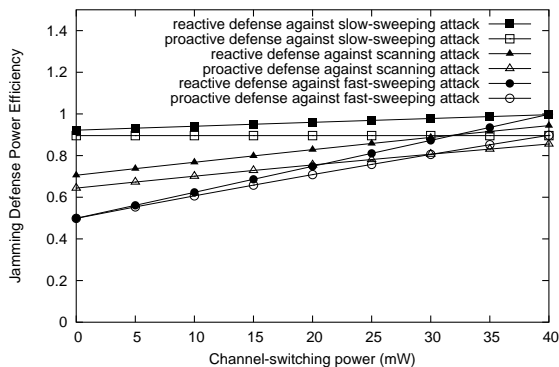


Figure 6: Effect of channel-switching power on JDPE. 3 radios and 12 channels.

Again, the *maximizer* defense strategy in this game is the one that solves the problem:

$$\arg \max_{d \in \mathcal{D}} \min_{a \in \mathcal{A}} JDPE(d, a, S)$$

The previous simulation analysis is used to determine the solution of the efficiency game. From Fig. 3, it is best for attackers to use the fast-sweeping attack, to cause the least JDPE, and in this case both reactive and proactive defenses perform the same.

This is confirmed at different numbers of channels. The fast-sweeping attack (bottom two lines in Fig. 4) is still the best attack strategy causing the worst JDPE. Even with 4 channels, although scanning attackers caused less JDPE when proactive defense was used, fast-sweeping attack achieved less JDPE when the best defense (reactive) was used.

From Fig. 5, when channel-hopping overhead is negligible (compared to packet-time), the best attack strategy is scanning and the best defense strategy is reactive. For the other delay values, fast-sweeping attack is best for attackers, and both reactive and proactive defenses perform the same.

An important observation is that there is a turnover in the best attack strategy as the number of jamming radios increased, as observed in Fig. 8. As the number of attack radios is below 6 (half the channels), the best attack strategy is fast-sweeping; it is scanning afterwards. The reason is that once attackers exceed half the channels, some of them do not need to move and waste time in channel-hopping.

From the previous analysis, the following conclusion is reached:

Under the studied system parameters, if the channel-hopping overhead is negligible or the number of attack radios far exceeds the number of communication radios, the Nash equilibria in the efficiency game in multi-radio networks is $\langle \text{reactive}, \text{scanning} \rangle$. Otherwise, there are two Nash equilibria: $\langle \text{reactive}, \text{fast-sweeping} \rangle$ and $\langle \text{proactive}, \text{fast-sweeping} \rangle$.

8. CONCLUSIONS

In this paper we generalized the software-based channel-hopping jamming defense into multi-radio wireless networks. We compared two defense strategies, namely proactive and reactive, against three attack strategies, namely scanning, slow-sweeping, and fast-sweeping. We modeled the jamming defense problem as a max-min game between defense and at-

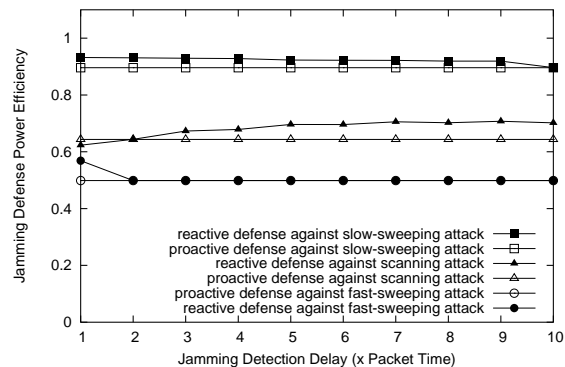


Figure 7: Effect of jamming-detection threshold on JDPE. 3 radios and 12 channels.

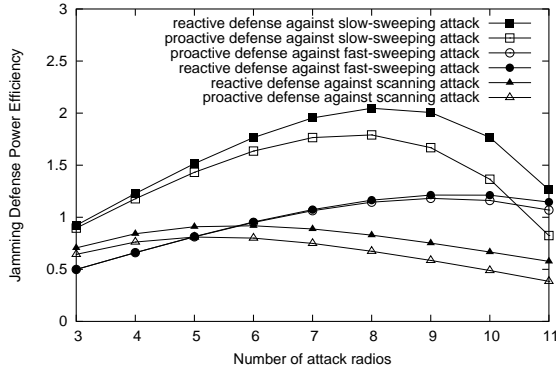


Figure 8: Effect of number of attack radios on JDPE. 3 communication radios.

tack and presented two variations of this game that differ in their payoff function.

Our results confirmed that proactive channel-hopping is a better alternative for single-radio networks; it is simpler to implement and achieves almost the same jamming resiliency as reactive channel-hopping. However, for multi-radio networks, reactive defense is more resilient to jamming. We based these conclusions on theoretical analysis for single-radio networks and on simulation experiments, in which we compared all defense-attack combinations under varying system parameters for multi-radio networks. For future work, we plan to complement our empirical evaluation of the studied jamming games with formal analysis of the Nash equilibria.

Acknowledgment

The authors would like to thank Taieb Znati for useful discussions during the early part of this research. This work is supported in part by NSF ITR medium ANI-0325353.

9. REFERENCES

- [1] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley Computer Publishing, 2001.
- [2] W. Xu, W. Trappe, and Y. Zhang, "Channel surfing: defending wireless sensor networks from interference," in *IPSN '07*, pp. 499–508.
- [3] A. D. Wood, J. A. Stankovic, and G. Zhou, "DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks," in *SECON '07*.
- [4] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in *INFOCOM '07*, pp. 2526–2530.
- [5] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan, "Understanding and mitigating the impact of rf interference on 802.11 networks," in *SIGCOMM '07*, pp. 385–396.
- [6] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *ACM MobiHoc*, 2005.
- [7] P. Bahl, A. Adya, J. Padhye, and A. Walman, "Reconsidering wireless systems with multiple radios," *SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 5, pp. 39–46, 2004.
- [8] A. D. Wood and J. A. Stankovic, "Denial of Service in Sensor Networks," *IEEE Computer*, vol. 35, no. 10, pp. 54–62, 2002.
- [9] G. Noubir, "On connectivity in ad hoc network under jamming using directional antennas and mobility," in *International Conference on Wired /Wireless Internet Communications, Lecture Notes in Computer Science*, Springer-Verlag, 2004.
- [10] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein, "Theory of spread spectrum communications—a tutorial," *IEEE Trans. Commun.*, vol. 20, pp. 855–884, May 1982.
- [11] Q. Wang, T. Gulliver, V. Bhargava, and E. Felstead, "Performance of Fast Frequency Hopped Noncoherent MFSK with a Fixed Hop Rate Under Worst Case Jamming," *IEEE Trans. Commun.*, vol. 38, pp. 1786–1798, 1990.
- [12] T. Gulliver and E. Felstead, "Anti-jam by Fast FH NCFSK - Myths and Realities," in *MILCOM '93*, pp. 187–191.
- [13] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Wormhole-based antijamming techniques in sensor networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 1, pp. 100–114, 2007.
- [14] Chipcon AS, "CC2420 2.4GHz IEEE 802.15.4 compliant RF Transceiver," <http://www.chipcon.com>, November 2003.
- [15] J. Polastre, R. Szewczyk, C. Sharp, and D. Culler, "The Mote Revolution: Low Power Wireless Sensor Network Devices," in *Hot Chips 16: A Symposium on High Performance Chips*, 2004.
- [16] P. Levis *et al.*, "The Emergence of Networking Abstractions and Techniques in TinyOS," in *NSDI '04*.
- [17] G. Noubir and G. Lin, "Low Power DoS Attacks in Data Wireless LANs and Countermeasures," *ACM SIGMOBILE Mobile Computing and Communications Review (MC2R)*, vol. 7, no. 3, 2003.
- [18] P. Bahl, R. Chandra, and J. Dunagan, "SSCH: slotted seeded channel hopping for capacity improvement in IEEE 802.11 ad-hoc wireless networks," in *MobiCom '04*, pp. 216–230.
- [19] A. Mishra, V. Shrivastava, D. Agrawal, S. Banerjee, and S. Ganguly, "Distributed channel management in uncoordinated wireless environments," in *MobiCom '06*, pp. 170–181.
- [20] G. Zhou, C. Huang, T. Yan, T. He, J. A. Stankovic, and T. F. Abdelzaher, "MMSN: Multi-Frequency Media Access Control for Wireless Sensor Networks," in *INFOCOM '06*.
- [21] Y. W. Law, L. van Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-efficient link-layer jamming attacks against wireless sensor network mac protocols," in *SASN '05*, pp. 76–88.
- [22] G. Alnife and R. Simon, "A multi-channel defense against jamming attacks in wireless sensor networks," in *Q2SWinet '07*, pp. 95–104.
- [23] A. D. Wood, J. A. Stankovic, and S. H. Son, "JAM: A Jammed-Area Mapping Service for Sensor Networks," in *RTSS '03*.
- [24] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service," in *WiSe '04*, pp. 80–89.
- [25] M. J. Osborne and A. Rubinstein, *A course in game theory*. MIT Press, 1994.