Modeling of the Channel-Hopping Anti-Jamming Defense in Multi-Radio Wireless Networks

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

Multi-radio (multi-interface, multi-channel) 802.11 and sensor networks have been proposed to increase network capacity and to reduce energy consumption, to name only a few of their applications. They are vulnerable, however, to jamming attacks, in which attackers block communication by radio interference or MAC-protocol violation. Two jamming countermeasures have been proposed, namely software-based channel hopping and error-correcting codes.

In this paper, we introduce the problem of maximizing network goodput under jamming attacks through a combination of channel hopping and error-correction coding. We describe the solution space and investigate one point thereof, namely *reactive defense against scanning attack*. We develop a Markovian model of the reactive channel-hopping defense against the scanning jamming attack and validate it using simulation experiments. Our results suggest that an adaptive defense, based on our model, would improve the resiliency of multi-radio networks against jamming.

Categories and Subject Descriptors

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

General Terms

Security, Reliability

1. INTRODUCTION

The wireless jamming attack aims at preventing sender nodes from accessing the shared wireless medium by keeping the medium busy or from successful reception by causing high radio interference at the receiver. Channel hopping, whereby the used radio channels are switched at the software-level, is an effective mechanism to mitigate jamming in wireless sensor networks and 802.11 networks. It has been proposed and evaluated in the context of *single-radio* networks, wherein each wireless node is equipped with a single radio interface [1, 2, 3, 4].

Advances in radio technology have also enabled the paradigm of *multi-radio* wireless networks, which have been proposed to increase overall network capacity by exploiting channel diversity [5]. For instance, multi-radio 802.11 nodes are equipped with multiple radio interfaces operating at orthogonal channels. The multiple radio interfaces can also be used to increase communication reliability by sending redundant data: either same data on different channels or encoding data and sending it in parallel through all channels. Clearly, reliability comes at the expense of reduced goodput. Understanding the trade-off between goodput and reliability is essential to make optimal utilization of the multiple radios.

This paper considers the problem of maximizing network goodput under jamming attacks in multi-radio networks by combining channel-hopping and error-correcting codes (ECC) [6]. Two factors affect goodput. First, high redundancy in ECC reduces goodput. Second, jamming may result in data loss if the number of clear (non-jammed) radios is smaller than the number necessary to recover transmitted data. However, these two factors are interestingly interdependent. Increasing ECC redundancy results in reduced goodput but also in increased jamming resiliency. This interlocking suggests the existence of optimal ECC redundancy that achieves maximum goodput. Noting that such optimal redundancy depends on system and attack parameters and that the attack strategy is not always known beforehand, an adaptive mechanism is needed to discover attack parameters and tune the ECC accordingly.

A first step in devising such an adaptive mechanism is modeling defense and attack strategies under different ECC parameters. Such model can be used to detect attack strategies given the known system and defense parameters. In this paper, we develop and validate models for different hopping strategies against different attack strategies, taking into consideration that the data is encoded to correct errors.

Our contributions can be summarized as follows:

- We introduce and formalize the problem of maximizing goodput under jamming in multi-radio networks using

MobiQuitous 2008, July 21-25, 2008, Dublin, Ireland.

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3604
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3604

(a) Quad-radio Wi-Fi Access Point. (www.hopling.nl)

(b) Sensor board with four attached radios. (www.atific.fi)

Figure 1: Examples of Multi-radio Wireless Devices.

combination of channel-hopping and ECC.

- We develop and validate (using simulation) models for different combinations of defense and attack hopping strategies. The models incorporate the effect of ECC redundancy on communication availability.

The rest of the paper is organized as follows. In the next section, we discuss background and related work. Section 3 presents the jamming defense problem in multi-radio networks and formalizes it as a goodput maximization problem. In Section 4, we present our models of different attack and defense hopping strategies. Section 5 presents our simulation results that we use to validate our models. We conclude in Section 6.

2. BACKGROUND AND RELATED WORK

We start by presenting background on the radio jamming problem, multi-radio networks, channel-hopping, and error-correcting codes.

2.1 Radio Jamming

Radio jamming is a DoS attack targeting physical and link layers of wireless networks [7, 8]. Other DoS attacks in wireless networks are modeled in [9]. Many anti-jamming techniques have been proposed, spanning many layers in the network stack. Physical-layer anti-jamming techniques, such as directional (sectored) antennas [10] and spread-spectrum [11], create hard-to-jam "virtual channels" or "wormholes" within the shared wireless medium [12, 13, 14]. Sectored antennas are potentially effective but not widely deployed. Although spread-spectrum radio chips have been deployed in new generations of sensors [15, 16, 17], these hardware-based techniques are still vulnerable to jamming from nodes with similar radios [2]. Moreover, the recent 802.11a and 802.11g standards have replaced the jamming tolerant, limited bandwidth frequency-hopping with high bandwidth channel coding schemes (e.g., OFDM) [3].

TDMA-based protocols and multi-frequency link-layer protocols, both static [18] and dynamic [19], mitigate low-power, selective jamming as long as the TDMA and frequency-switching schedules are secure. To mitigate schedule compromise, data blurting with schedule switching [20] and data exfiltration (by time-multiplexing redundant data over multiple channels) [21] have been proposed.

The Jammed-Area Mapping (JAM) scheme [22] identifies regions of jammed sensors to be avoided by routing protocols. Jammed sensors turn themselves into sleep mode to outlast jammers. 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 [23]. Our work differs in that the goal is to allow jammed nodes to communicate *while* the jamming attack is on.

All previous work studies jamming in the context of single-radio networks. Our work investigates jamming mitigation in the multi-radio context and studies optimal interaction between channel hopping and data redundancy enabled by the availability of multiple radios. We generalize channel-hopping to multi-radio networks and present the first investigation of different redundancy and hopping tactics in these networks and their cost-benefit trade-offs under varying adversarial conditions.

2.2 Multi-radio Networks

Multi-radio wireless networks have been proposed to increase overall network capacity by exploiting channel diversity [5]. For instance, multi-radio 802.11 mesh nodes (as in Figure 1(a)) are equipped with multiple radio interfaces operating at orthogonal channels to decrease interference between parallel streams of data at different radio channels. Also, sensors equipped with multiple radio chips (e.g., Figure 1(b)) are used to increase throughput and/or reliability.

2.3 Channel Hopping

Channel hopping, whereby channel switching is controlled at the software-level, has been proposed to mitigate jamming in *single-interface* wireless sensor networks (WSNs) and 802.11 networks [1, 2, 3, 4]. 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 [3], 802.15.4 (e.g., CC2420 radio in MICAz motes) has 16 channels [2], and even the older CC1000 radio in Mica2 motes has been reported to allow up to 32 orthogonal channels in the 900MHz band [1]. We have experimented with 4 orthogonal channels on the Mica2 motes in the 433MHz band, 3 channels on 802.11b/g, and 13 channels on 802.11a. In all these standards, a radio cannot transmit or receive while switching channels.

Different values of the channel-residence time have been used to serve different purposes. Whether channel hopping is implemented at the driver or user levels has an effect on the attainable granularity of the channel-hopping frequency. Channel hopping has been implemented to occur every few microseconds [2], enough to send a small packet fragment, few milli-seconds [19, 4], hundred milli-seconds [3], and few seconds [24]. Wood *et al.* show that the packet fragment time should be small (in the order of channel-hopping delay) to prevent a fast-switching attacker from disrupting communication on all channels [2]. We follow their recommenda-

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3604
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3604

tion and use short packets (in the same order as channel-switching delay) in our approach.

Proactive channel-hopping has been shown to improve resiliency to jamming in both 802.11 [3, 4] and sensor networks [2]. Against static and scanning attackers, channel hopping was enough to improve throughput in 802.11a and 802.11b networks [3, 4]. However, against pulsing, fast-switching attackers, channel hopping was not enough; packet fragmentation and redundant encoding were needed to defend against this type of jamming [2]. Channel hopping is coordinated synchronously [3, 4, 2] requiring loose clock synchronization. Asynchronous channel hopping has also been proposed but only for low-bandwidth message delivery [14]. 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 [1].

Again, previous channel-hopping research has only considered channel hopping in single-radio networks. Our work generalizes the channel-hopping technique to multi-radio networks and studies its interaction with data redundancy using ECC.

2.4 Error-correcting Codes (ECC)

Error-correcting codes (ECC) and cryptographic bit interleaving have been proposed to mitigate low-power jamming attacks against data networks [25]. Alone, these techniques are not effective against high power or link-layer jammers. They also incur unnecessarily high communication and processing overhead if care is not taken in selecting the optimal ECC parameters. Our work introduces the problem of optimizing the ECC by combining it with channel-hopping.

Generally in ECC, the piece of data to be transmitted reliably is augmented with carefully-designed redundancy, and the augmented data divided into a number of pieces, n, which then get transmitted over the unreliable communication channel. Finally, the original piece of data can be recovered from any combination of m out of the n pieces. The ECC is usually described as a tuple (n, m). The *goodput* of the communication channel is reduced by the amount of redundancy. In particular, in the IDA algorithm, goodput is $\frac{m}{n}$ of the channel throughput [6].

3. JAMMING DEFENSE IN MULTI-RADIO NETWORKS

In this section, we present the problem of maximizing network goodput under jamming using a combination of channel-hopping and ECC. We start by describing the system and attack models, followed by a formulation of the problem, and finally a description of the reactive hopping defense strategy studied in this paper.

3.1 System Model

In multi-radio wireless networks, each node is equipped with a number, n_f, of radio interfaces, each of which operates at one of n_h orthogonal (different, non-interfering) radio channels. As described in Section 2.3, many wireless standards support multiple orthogonal channels.

Each piece of data to be transmitted is encoded using an (n_f, m) IDA ECC [6]; because the number of encoded data pieces is the same as the number of radios, each piece of data is then transmitted over a different radio interface. A data piece is lost if more than $n_f - m$ radios are jammed, because there would not be enough non-faulty pieces to recover the data (recall that any combination of at least m pieces can be used to reconstruct the transmitted data).

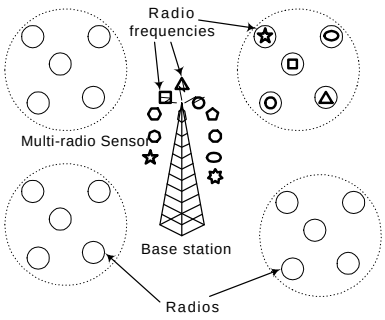

Figure 2: An example multi-radio wireless network. Radios in multi-radio sensors communicate with the base-station over orthogonal channels. The figure depicts four sensors with five radios in each sensor ($n_f = 5$) and a total of ten channels ($n_h = 10$). The base-station is equipped with ten wireless transceivers to cover the full spectrum.

Fig. 2 depicts an example architecture of a multi-radio wireless sensor network, whereby multi-radio sensors have 5 radios each, and all radios in a sensor act as a single unit (they are embedded into a single device). Radios in each sensor send encoded data to the base-station over 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 as will be described in Subsection 3.3. Although the number of transceivers at the base-station can be large (e.g., 12 in 802.11a), the base-station is a single node in the network and is usually well-equipped. However, we believe that this assumption can be relaxed without significant impact on our results. Medium access is scheduled between sensors using TDMA. For simplicity of presentation, in what follows only one sensor is considered. Radios hop among the channels according to the defense strategy in effect.

3.2 Attack Model

The jamming attack against multi-radio networks is launched by a number of attack radios, n_x, that is less than the total number of channels, n_h, and each attack radio can jam one channel at a time. While a channel is jammed, no data can be communicated on that channel. For instance, a compromised sensor can jam communication by overriding the MAC-protocol and sending packets continuously (low-power attack methods are also feasible [8]). Because the compromised sensor uses the same Spread Spectrum (SS) [11] channel (if SS is used) as the attacked sensors, SS by itself cannot prevent this jamming attack.

Scanning Attack. Scanning attackers hop between channels so that the set of jammed channels change over time.

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3604
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3604

Scanning attackers sense legitimate channel activity to determine if the channel they jam is being used. Each attacker radio keeps hopping until it finds a channel that has legitimate activity, and the attacker stays there until no activity is detected. It takes an attacker a certain delay, *channel-sensing-time*, to determine channel activity or lack thereof. This delay depends on the legitimate traffic rate and on how frequently the attacker stops jamming to sense the medium activity.

Two variations of the scanning attack are modeled, namely *exploratory* and *conservative*. In the exploratory-scanning attack, jammers at unused channels select the next target channels randomly from the set of unjammed channels, whereas in the conservative-scanning attack, jammers at unused channels select their next targets randomly from a set containing all channels (including currently jammed channels) in anticipation of the *deceptive defense* described below.

3.3 Reactive Hopping

In the reactive hopping defense 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. The new channel is selected uniformly at random using a securely seeded random-number generator. Jamming may keep the wireless medium busy, resulting in a long waiting-time to access the channel, or may corrupt packets by causing high interference at the receiver, resulting in excessive failed transmissions. In our model, only the sender has to detect jamming and decide to switch channels. The receiver (the base-station in Figure 2) does not need to be informed explicitly with the channel-switching decisions as it is already listening on all the channels.

We use a simple jamming detection algorithm: if the waiting-time for a free channel or the number of consecutive, unsuccessful transmission attempts exceeds a threshold, jamming is assumed and the radio hops to a different channel. We note that this detection algorithm is simpler than other detection approaches presented in the literature. For instance, in the DOMINO MAC-misbehavior detection system, the access point identifies misbehaving stations by monitoring frame retransmissions and backoff values [26]. To reduce false detection, the monitoring period used was ten seconds. Our detection algorithm makes no attempt to identify misbehaving nodes, and it is run at the sender node only.

We note that the jamming-detection threshold is usually much longer than the channel-hopping delay, that is, the time taken by the radio to switch channels. Channel-switching times of tens of micro-seconds have been reported (e.g., [19, 2]), whereas the jamming detection can take up to seconds [8]. Based on this large gap, we set the hopping overhead to zero in the models presented in Section 4, and the jamming-detection and attack channel-sensing delays to one time-slot each. In the simulation study in Section 5, we use more realistic delay values.

Two variations of the reactive defense are modeled, namely *straightforward* and *deceptive*. In the straightforward reactive defense, jammed radios select the next target channels randomly from the set of unused channels, whereas in the deceptive reactive defense, jammed radios select their next channels randomly from a set containing all channels (including currently used channels).

It should be noted that another alternative is proactive channel-hopping, whereby radios periodically switch channels regardless of jamming detection [2, 3, 4]. Proactive channel-hopping is simpler to implement, because it does not require jamming detection. However, it has been recently shown that reactive channel-hopping achieves better jamming tolerance than proactive in multi-radio networks [27].

3.4 Maximizing Network Goodput

As mentioned previously, ECC reduces the goodput by the code rate $\frac{m}{n_f}$, where n_f is the number of radios. Furthermore, jamming reduces goodput of an ECC-encoded channel by blocking communication at more than $n_f - m$ radios. Let P_{block} represent the jamming-induced *blocking probability*, or the probability that more than $n_f - m$ radios are jammed at the same time, resulting in data loss. The goodput (as a fraction of the maximum throughput achievable in the absence of jamming) of the multi-radio channel can then be formulated as:

$$goodput = \frac{m}{n_f}(1 - P_{block})$$

The multi-radio channel under jamming can be viewed as a time sequence of decisions (by jammers and defenders) on which channels to operate their radio interfaces. Assume that we have n_h channels so that the defense and attack decision vectors are modeled as n_h-bit vectors, each bit corresponding to whether the corresponding channel is used by the jammers or defenders, respectively. Because the number of used channels at any time slot cannot exceed the number of radio interfaces, the number of 1-bits in each vector is at most n_f for the defenders and n_x for the jammers. The space of defense and attack hopping strategies is all the possible time sequences of decision vectors. However, due to channel-switching delays, some sequences are not feasible, particularly those with the time distance between channel switching being less than the switching delay. Depending on the overlap of jammed and communication channels, and the coding scheme used by the defenders, the probability of the communication being blocked can be calculated.

We note the relation between m, representing the amount of redundancy of the ECC, and the blocking probability, P_{block}. As m decreases, and correspondingly, the amount of redundancy required in each encoded piece increases, it becomes harder for jammers to cause data loss, and hence, the blocking probability decreases. The amount of decrease of the blocking probability and the resulting net effect on goodput depend on the hopping and jamming strategies as well as the number of channels.

Considering the problem of maximizing goodput, the solution space encompasses the selection of the coding parameter m and the hopping strategy. Because the goodput also depends on the adversarial attack strategy, which may not be always known beforehand, a mechanism is needed to discover the attack parameters, particularly the attack strategy and the number of attackers, and adjust the defense param-

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3604
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3604

eters, particularly the coding parameters, number of radios, and hopping strategy, accordingly. A main building block of such mechanism is a model that captures the interaction between defense, attack, and system parameters. Building this model is the focus of the next section.

4. MARKOVIAN MODELS

This section presents models to derive the blocking probability given defense, attack, and system parameters. The main envisioned usage of this model is to drive an adaptive mechanism that infers the otherwise unknown attack parameters and adjusts the defense parameters to maximize goodput. To this end, Markov Chains are used to model reactive defense and scanning attack in multi-radio networks. A Markov chain is represented by a set of states and transition probabilities, p_{ij}, between these states. In these models, each state represents the number of jammed radios, ranging from 0 to n_f. Therefore, there are $n_f + 1$ states.

From the steady-state probabilities $\pi_i, i = 0, 1, \cdots, n_f$, the blocking probability can be derived given the parameters of the ECC in effect. For an (n_f, m) ECC, the blocking probability is the sum of the steady-state probabilities of states in which more than $n_f - m$ radios are jammed. That is, $P_{block} = \sum_{i=n_f-m+1}^{n_f} \pi_i$.

To solve the Markov model, the transition-probability matrix, $[p_{ij}]$, is derived. The steady state probabilities can then be derived using the standard matrix equations:

$$[\pi_i][p_{ij}] = [\pi_i] \quad \text{and} \quad \sum_{i=0}^{n_f} \pi_i = 1$$

The models assume instantaneous channel hopping, that is, the delay of switching channels is 0, and that the delay of detecting jamming (for defense) and sensing channel activity (for attack) is one time slot.

The *drawing without replacement* formula is extensively used in the models, and hence a shortcut is used:

$$DWR(a, b, c, d) = \frac{\binom{b}{d}\binom{a-b}{c-d}}{\binom{a}{c}}$$

$DWR(a, b, c, d)$ is the probability that c drawings (without replacing the drawn members) from a population of size a, of which b are distinguished, yield exactly d distinguished members. $\binom{x}{y}$ is the binomial coefficient of x and y, also called "x choose y".

In what follows, state i represents the state where i of the n_f radios are jammed as depicted in Fig. 3. All the jammed i radios hop channels in the next time-step. In the straightforward defense, the i radios randomly select the next target channels from among the unused $n_h - n_f$ channels, whereas in the deceptive defense, the i radios select their next channels from both the unused channels as well as their current channels. It should be noted, however, that in straightforward defense, if i is larger than $n_h - n_f$, then there are not enough unused channels for all the i jammed radios to move to, and hence, $\ell = i - (n_h - n_f)$ (randomly selected) of the i jammed radios are forced not to hop, while the remaining $i - \ell$ hop to new channels.

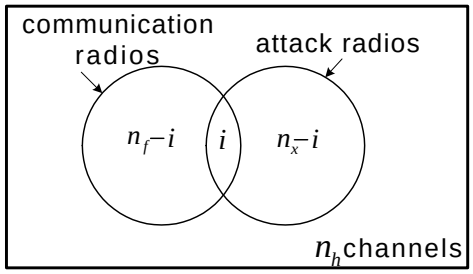

Figure 3: Communication and attack radios at state i (i jammed radios).

Similarly, when transitioning out of state i, all the $n_x - i$ attack radios that are not successfully jamming active channels will move to new channels. In the exploratory attack, the $n_x - i$ attack radios randomly select the next target channels from among the unjammed $n_h - n_x$ channels, while in the conservative attack, the $n_x - i$ attack radios select their next channels from both the unjammed channels as well as their current channels. It should be noted, however, that in exploratory attack, if $n_x - i$ is larger than $n_h - n_x$, then there are not enough unjammed channels for all the $n_x - i$ attack radios to move to, and hence, $\ell_x = (n_x - i) - (n_h - n_x)$ (randomly selected) of the $n_x - i$ attack radios are forced not to hop, while the remaining $n_x - i - \ell_x$ hop to new targets.

The following four theorems present formula for the transition probabilities p_{ij} for the four attack-defense combinations.

THEOREM 1. *For a* straightforward reactive defense vs. conservative scanning attack *with no channel-hopping overhead, the transition probability p_{ij} is:*

$$p_{ij} = DWR(n_h - i, n_f - \ell, n_x - i, j - \ell)$$

where n_x is the number of attackers, n_f the number of communication radios, n_h the number of channels, and $\ell = max(0, i - (n_h - n_f))$.

PROOF. At state i, all the jammed i radios hop channels in the next time-step. However, $\ell = max(0, i - (n_h - n_f))$ radios have to stay put in their current channels if there are not enough new channels to hop to, where ℓ is the difference between the i radios that need to hop and the $n_h - n_f$ available unused channels, that is, $\ell = max(0, i - (n_h - n_f))$. Meanwhile, $n_x - i$ attackers detect that their channels are unused and select new channels out of $n_h - n_x$ unjammed channels plus the previously-jammed $n_x - i$ for a total of $n_h - i$ channels in the next time-step.

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3604
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3604

In the next time-step, ℓ radios are already jammed because they have to stay put in the jammed channels. Thus, to jam a total of j radios, the $n_x - i$ hopping attackers have to jam exactly $j - \ell$ radios. The probability of this event is derived using drawings-without-replacement:

$$DWR(n_h - i, n_f - \ell, n_x - i, j - \ell)$$

where the hopping attackers draw $n_x - i$ channels out of $n_h - i$ channels with $n_f - \ell$ of them used by communication radios. □

Intuitively, the first component of the next formula represents deceptive-reactive communication radios selecting their next channels from the ones they currently use, and thus, stay jammed. The second component represents the probability that attack radios jam enough radios to cause exactly j jammed radios in the next time slot.

THEOREM 2. *For a* deceptive reactive defense vs. conservative scanning attack *with no channel-hopping overhead, the transition probability p_{ij} is:*

$$p_{ij} = \sum_{o=o_{min}}^{o_{max}} DWR(n_h - (n_f - i), i, i, o) \cdot$$
$$DWR(n_h - i, n_f - o, n_x - i, j - o)$$

where $o_{min} = max(0, j - (n_x - i))$, and $o_{max} = min(i, j)$.

PROOF. At state i, all the jammed i radios hop channels in the next time-step and select from the $n_h - n_f$ unused channels plus their current i channels. Let o radios hop to channels from the previously-used i channels. The probability of this event is:

$$p_o = DWR(n_h - (n_f - i), i, i, o)$$

where radios draw i channels out of $n_h - n_f + i$ channels, i of them active in the previous time-step.

Meanwhile, $n_x - i$ attackers detect that their channels are unused and hop to channels selected out of the $n_h - i$ unjammed channels.

In the next time-step, o radios are their jammed because they stay at already-jammed channels. Thus, to jam a total of j radios, the $n_x - i$ hopping attackers have to jam exactly $j - o$ radios. The probability of this event is:

$$p = DWR(n_h - i, n_f - o, n_x - i, j - o)$$

where the hopping attackers draw $n_x - i$ channels out of $n_h - i$ channels with $n_f - o$ of them used by communication radios.

To compute the overall transition probability, note that the sample space is partitioned based on o, the number of radios falling into the i channels. Therefore, the transition probability is computed as follows: $p_{ij} = \sum_o [p_o \cdot p]$. Substituting in this equation yields the formula presented in the theorem. The summation limits o_{min} and o_{max} are computed by solving the constraints for each combination x choose y: that both x and y are ≥ 0 and that $x \geq y$. □

Intuitively, the first and second components of the next formula represent exploratory-reactive communication radios escaping from their jammed channels but ending up selecting their next channels where attack radios stay because they do not have enough unjammed channels to move to. The third component represents the probability that attack radios end up jamming j radios in the next time slot.

THEOREM 3. *For a* straightforward reactive defense vs. exploratory scanning attack *with no channel hopping overhead, the transition probability p_{ij} is:*

$$p_{ij} = \sum_{k=k_{min}}^{k_{max}} DWR(n_h - n_f, n_x - i, i, k) \cdot$$
$$\sum_{m=m_{min}}^{m_{max}} DWR(n_x - i, \ell_x, k, m) \cdot$$
$$DWR(n_h - n_x, n_f - \ell - k, n_x - i - \ell_x, j - \ell - m),$$

where $\ell_x = max(0, n_x - i - (n_h - n_x))$, $k_{min} = max(0, n_f + n_x - n_h - \ell)$, $k_{max} = min(n_x - i, i - \ell)$, $m_{min} = max(0, i - \ell - n_h + n_f + \ell_x, j - n_f + k, i - n_x + \ell_x + j - \ell, k - n_x + i + \ell_x)$, and $m_{max} = min(k, \ell_x, j - \ell, n_h - 2n_x - n_f + k + i + j + \ell_x)$.

PROOF. All the jammed i radios at state i hop channels in the next time-step. They select new channels out of the unused $n_h - n_f$ channels. However, it may be the case that there are not enough new channels to accommodate all hopping radios, and ℓ of them have to stay put in their current channels.

Also, some radios hop to channels in the $n_x - i$ channels that were occupied by the rest of the attackers. The probability that k radios fall on these $n_x - i$ channels is: $p_k = DWR(n_h - n_f, n_x - i, i, k)$, where radios draw i channels out of $n_h - n_f$ channels with $n_x - i$ jammed in the previous time-step.

Meanwhile, $n_x - i$ attackers detect that their channels are unused and hop to new channels (out of the $n_h - n_x$ unjammed channels) in the next time-step. But, it may be the case that there are not enough new channels to accommodate all hopping attackers. The number of attackers that have to stay put is ℓ_x, where ℓ_x is the difference between the $n_x - i$ attackers that need to hop and the $n_h - n_x$ available unjammed channels, that is, $\ell_x = max(0, n_x - i - (n_h - n_x))$.

In the next time-step, ℓ radios are already jammed because they have to stay put in the jammed channels, and some of

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3604
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3604

the k radios that hopped to the $n_x - i$ channels previously occupied by attackers may be jammed as well if they coincide with the ℓ_x attackers that have to stay put. Let the number of radios that fall into the ℓ_x channels be denoted as m.

The probability that m radios fall on the ℓ_x staying attackers given that k radios hop to the previously-jammed $n_x - i$ channels is: $p_m = DWR(n_x - i, \ell_x, k, m)$, where radios draw k channels out of $n_x - i$ channels with ℓ_x jammed by staying attackers. The rest of the k radios are not jammed, because there are no other attackers in the $n_x - i$ channels except the ℓ_x attackers.

On the attack side, there are $n_x - i - \ell_x$ attackers that hopped their channels in search of used channels out of $n_h - n_x$ channels. Because $\ell + m$ radios are already jammed, all that these attackers have to do now in order to jam a total of j radios is to jam $j - \ell - m$ radios from the rest of the radios $(n_f - \ell - k)$. The probability that the hopping attackers jam *exactly* $j - \ell - m$ radios is: $p_{km} = DWR(n_h - n_x, n_f - \ell - k, n_x - i - \ell_x, j - \ell - m)$, where the hopping attackers draw $n_x - i - \ell_x$ channels out of $n_h - n_x$ channels with $n_f - \ell - k$ used by communication radios.

The sample space is partitioned based on k, the number of radios falling into the $n_x - i$ channels. The space is partitioned further by m, the number of radios falling into the staying attackers. Therefore, the transition probability is computed as follow: $p_{ij} = \sum_k [p_k \cdot \sum_m [p_m \cdot p_{km}]]$. Substituting in this equation yields the formula presented in the theorem. Again, the summation limits k_{min}, k_{max}, m_{min}, and m_{max} are computed by solving the constraints for each choose combination. □

Intuitively, the first component of the next formula represents jammed radios that stay jammed because they end up staying at their current channels. The second and third components represent jammed radios that stay jammed because they escape to channels jammed by attack radios that do not have enough channels to move to. The fourth component represents the probability that attack radios jam enough radios to cause exactly j jammed radios in the next time slot.

THEOREM 4. Deceptive reactive defense vs. exploratory scanning attack. *The transition probability p_{ij} for deceptive reactive defense and exploratory scanning attack with no channel hopping overhead is:*

$$p_{ij} = \sum_{o=o_{min}}^{o_{max}} DWR(n_h - (n_f - i), i, i, o) \cdot$$

$$\sum_{k=k_{min}}^{k_{max}} DWR(n_h - n_f, n_x - i, i - o, k) \cdot$$

$$\sum_{m=m_{min}}^{m_{max}} DWR(n_x - i, \ell_x, k, m) \cdot$$

$$DWR(n_h - n_x, n_f - o - k, n_x - i - \ell_x, j - o - m)$$

where $o_{min} = max(0, i - (n_h - n_f), n_f - n_h)$, $o_{max} = i$, $k_{min} = max(0, n_f - n_h + n_x - o)$, $k_{max} = min(n_x - i, i - o, n_f - o)$, $m_{min} = max(0, j - n_f + k, k - n_x + i + \ell_x, j - o + n_x + i + \ell_x)$, *and* $m_{max} = min(k, \ell_x, j - o, n_h - 2n_x - n_f + i + \ell_x + j + k)$.

PROOF. At state i, all the jammed i radios hop channels in the next time-step. Instead of selecting all new channels, they hop to channels out of the unused $n_h - n_f$ channels plus their current i channels. Let o radios select their channels from the i channels previously used. As previously discussed, the probability of this event is: $p_o = DWR(n_h - (n_f - i), i, i, o)$.

Also, let k of the remaining $i - o$ radios, which now select their channels out of only the unused $n_h - n_f$ channels, hop to channels from the $n_x - i$ channels occupied by the rest of the attackers. The probability of this event is: $p'_k = DWR(n_h - n_f, n_x - i, i - o, k)$, where radios draw $i - o$ channels out of $n_h - n_f$ channels with $n_x - i$ jammed in the previous time-step. On the other side, $n_x - i$ attackers detect that their channels are unused and hop to new channels (out of the $n_h - n_x$ unjammed channels) in the next time-step. Also, ℓ_x attackers stay put because there is not enough new unjammed channels.

In the next time step, o radios are already jammed because they stay put at the jammed i channels. Let m radios, out of the k that hop to the $n_x - i$ channels previously occupied by attackers, coincide with the ℓ_x attackers that have to stay put. These m radios will be jammed as well. As previously discussed, the probability of this event is: $p'_m = DWR(n_x - i, \ell_x, k, m)$. The probability that the $n_x - i - \ell_x$ hopping attackers jam *exactly* $j - o - m$ radios is: $p_{okm} = DWR(n_h - n_x, n_f - o - k, n_x - i - \ell_x, j - o - m)$, where the hopping attackers draw $n_x - i - \ell_x$ channels out of $n_h - n_x$ channels with $n_f - o - k$ used by communication radios.

The sample space is partitioned based on o, the number of radios falling into the i channels. The space is partitioned further by k, the number of radios falling into the previously-jammed $n_x - i$ channels, and further by m, the number of radios falling into the ℓ_x staying attackers. Therefore, the transition probability is computed as follows: $p_{ij} = \sum_o [p_o [\sum_k [p'_k \cdot \sum_m [p'_m \cdot p_{okm}]]]]$. Substituting in this equation yields the formula presented in the theorem. The summation limits o_{min}, o_{max}, k_{min}, k_{max}, m_{min}, and m_{max} are computed simply by solving the constraints for each choose combination. □

5. SIMULATION ANALYSIS AND MODEL VALIDATION

We conducted a simulation-based study using a home-grown simulator to validate the models presented in the previous section. The simulator models the reactive defense and scanning attack strategies and captures the same model assumptions used in deriving the theoretical results except for the negligible hopping delay assumption, as will be described shortly. Simulation time is divided into slots, where each time slot represents the time to transmit one piece of ECC-encoded packets, or what we call the *packet-time*. The default ECC used in the simulation is $(n_f, 1)$, that is, any piece

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3604
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3604

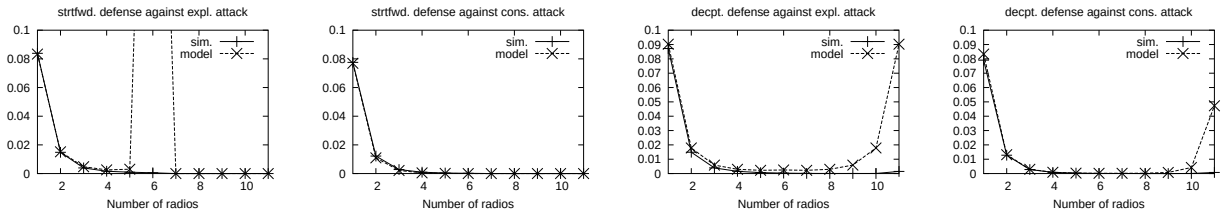

Figure 4: Effect of number of communication and attack radios on blocking probability. 12 channels.

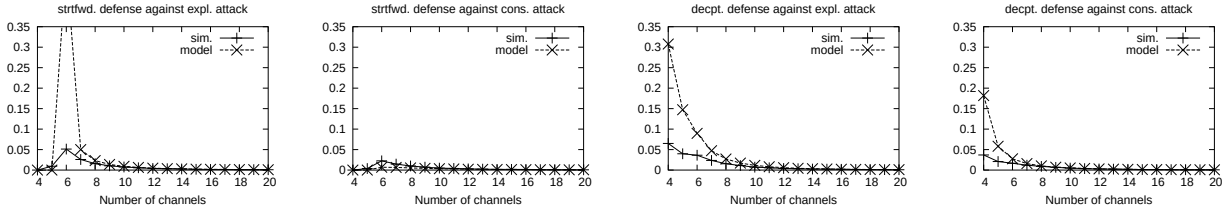

Figure 5: Effect of number of channels on blocking probability. 3 radios.

Table 1: Defense and attack parameter values used in the simulations (Bold face represents default values)

Parameter	Values
Number of pieces needed to correct errors (m)	[1-3], **1** (full replication)
Number of channels	[4-20], **12**
Number of radios	[1-11],**3**
Number of attackers	[1-11],**3**
Channel-hopping delay	**1** packet-time
Jamming-detection threshold	**10** packet-time
Attacker channel-sensing time	**10** packet-time

of encoded data is enough to recover the original data, and correspondingly, the blocking probability is the percentage of time *all* radios are jammed.

Table 1 summarizes the parameters used. We varied the number of channels from 4 as in CC1000 radio in the 433MHz band up to 20 with a default value of 12 as in 802.11a. We varied the number of radios from 1 to 11 with a default value of 3, and we set the number of attack radios to be the same as the number of defense radios unless otherwise specified. We use the packet-time as the unit for time-based parameters. To examine the effect of the model assumption of negligible hopping delay, we set the channel-hopping delay to 1 packet-time (instead of 0 packet-time in the model), and both the jamming-detection threshold and the attack channel-sensing time to 10 packet-time (instead of 1 packet-time in the model)[1]. Each experiment run lasts for about one million packet-time, and we report the average of 10 runs. The 90% confidence intervals were smaller than 2% of the average reported at each data point.

For all the tests, as can be seen from the figures, the model matched the simulation results almost exactly for most of the studied parameter range.

Effect of number of communication and attack radios. In the first set of experiments, we varied the number of radios per communication node and changed the number of attack radios to match the number of communication radios. As shown in Fig. 4, as more radios per node are used, the blocking probability decreases. A notable difference between simulation results and the model occurred in the deceptive defense strategy against both attack strategies (the two rightmost graphs in Fig. 4) when the number of radios is very close to the number of channels (12 channels in this experiment). We hypothesize that this discrepancy occurs as channel hopping occurs more frequently (many radios with less room to escape) and the effect of the non-zero hopping delay (compared to 0 delay in the model) becomes more pronounced.

Another point where simulation results differed from the model prediction is the bump in straightforward defense against exploratory attack (leftmost graph in Fig. 4). In the straightforward-exploratory combination, the blocking probability is predicted by the model to increase to 0.5 at 6 radios[2]. This bump occurs at a number of radios exactly half of the number of channels. The reason is that at this number the system alternates between all radios being jammed in one time slot followed by all radios free in the next and so on. This alternation happens because at each time slot, the only option for communication (attack) radios is to hop to the other half of channels. We hypothesize that this bump did not occur in the simulations because the non-zero hop-

[1]In our simulator validation, we also ran the simulations with values corresponding to the model and obtained exactly the same results as the models; curves are not shown because they would be redundant and not contribute to the paper.

[2]A similar bump can also be observed in Fig. 5 (leftmost graph) at 6 channels with the number of radios per node being 3 in that experiment.

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3604
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3604

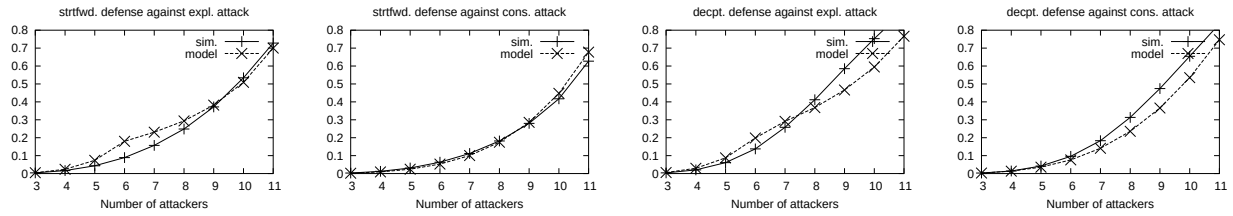

Figure 6: Effect of number of attack radios on blocking probability. 3 communication radios, 12 channels.

ping delay breaks this synchronized alternation. This alternation is not predicted in conservative attack (and deceptive defense) because conservative attack (deceptive defense) radios have also the option of choosing their next channels also from the ones they currently use.

Effect of number of channels. In the second experiment, we varied the total number of channels while fixing the number of radios and attackers at three. Fig. 5 shows that, as expected, with more channels the blocking probability decreased except for the bump in the straightforward defense (in the model only as explained above) at a number of channels twice that of radios per node, similar to the case above. The straightforward defense exhibits superior performance at low number of channels (except for the critical number of twice the number of radios).

Effect of number of attack radios. In the third experiment, we varied the number of attack radios while fixing the number of communication radios at three and the number of channels at 12. As expected, the blocking probability increases with increasing number of attack radios. The straightforward defense achieves slightly better performance at high number of attackers.

Simulation results differed from model prediction at high number of attackers only in the deceptive defense. Note that the model is otherwise more conservative than the simulation results, predicting a higher probability of jamming in most cases. At high number of attackers, deceptive radios hop more frequently, emphasizing the effect of the non-zero hopping delay. The straightforward radios escape from jamming slightly better, and, thus, they experience less hopping.

In summary, exploratory attacks are more effective in all cases, and straightforward defense is more effective except when the number of radios is half that of the channels.

Using the model. In the last experiment, we varied the ECC parameters, in particular the number of encoded data pieces required to recover from errors. In this experiment, we simulated the straightforward defense against the exploratory attack, as our results above indicate that these strategies are superior for the defense and attack, respectively.

In Figure 7 we show goodput results for 3 communication radios, 12 channels, and varied the number of attack radios to examine the effect of attack parameters on the optimal ECC. The best ECC depends on the number of attackers, which can be predicted by our models and confirmed by the simulation. Up to 6 attack radios, $(3, 2)$ ECC achieved

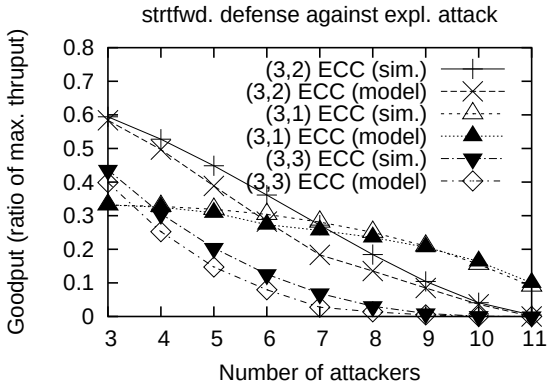

Figure 7: The best ECC redundancy depends on the number of attack radios. 3 communication radios, 12 channels, straightforward defense against exploratory attack.

the best goodput (as a ratio of the maximum throughput in absence of jamming). With more than 6 radios, full-replication, or $(3, 1)$ ECC, achieved the highest goodput.

The number of attack radios cannot always be known beforehand. We use our models to discover the number of attack radios and adjust the ECC parameters accordingly to achieve the best goodput. Periodically, the goodput is measured and fed into our models to predict the number of attack radios. This can be visualized as a horizontal line at the measured goodput value that intersects the model curve of the currently used ECC parameters. The x-value of the intersection represents a good estimate of the actual number of attack radios, which can be used in a feedback loop to adjust the ECC parameters optimally. For instance, if the ECC used is $(3, 2)$, and the goodput is measured as 0.4 from the maximum achievable throughput, then from the $(3, 2)$ ECC (model) curve in Fig. 7, the number of attack radios can be estimated as 5. Because the $(3, 2)$ ECC is still optimal at 5 attack radios, no change is needed. However, if the goodput is measured as < 0.2, the number of attack radios is estimated as > 7, and the ECC has to be changed to $(3, 1)$.

6. CONCLUSIONS

In this paper, we considered the problem of jamming defense in multi-radio networks, wherein each node is equipped with more than one radio interface. Our approach is to combine the software-based channel hopping with error-correcting

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3604
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3604

codes (ECC). We defined the problem of maximizing network goodput and illustrated the inter-dependency between ECC redundancy and jamming-induced blocking probability, suggesting the existence of an optimal ECC redundancy. The optimal ECC depends not only on system parameters, such as the number of radio interfaces and radio channels, but also on the defense hopping strategy, number of attackers, and attack hopping strategy.

We then developed models for reactive defense strategies against scanning attack strategies under varying ECC parameters. These models allow us to derive the blocking probability given the attack and defense hopping strategies, the number of channels, communication radios, and attack radios. We validated our models using simulation experiments. These models can also be used to detect attack parameters, if unknown, from measured blocking probability and known defense and system parameters. This detection opens the door for an adaptive defense mechanism that adjusts its parameters on the fly as attack parameters change. The development of such adaptive defense and its evaluation using real testbed experiments are subjects of future work.

Acknowledgments

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 and ANI-0524634.

7. REFERENCES

[1] W. Xu, W. Trappe, and Y. Zhang, "Channel surfing: defending wireless sensor networks from interference," in *IPSN '07*, 2007, pp. 499–508.

[2] 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*, June 2007.

[3] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in *INFOCOM*, 2007, pp. 2526–2530.

[4] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan, "Understanding and mitigating the impact of rf interference on 802.11 networks," in *SIGCOMM '07*, 2007, pp. 385–396.

[5] 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.

[6] M. O. Rabin, "Efficient dispersal of information for security, load balancing, and fault tolerance," *J. ACM*, vol. 36, no. 2, pp. 335–348, 1989.

[7] A. D. Wood and J. A. Stankovic, "Denial of Service in Sensor Networks," *IEEE Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[8] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *ACM MobiHoc*, 2005.

[9] Q. Huang, H. Kobayashi, and B. Liu, "Modeling of Distributed Denial of Service (DDoS) Attacks in Wireless Networks," in *IEEE 2003 Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM)*, 2003.

[10] 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.

[11] 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.

[12] 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.

[13] T. Gulliver and E. Felstead, "Anti-jam by Fast FH NCFSK - Myths and Realities," in *MILCOM'93*, 1993, pp. 187–191.

[14] 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.

[15] Chipcon AS, "CC2420 2.4GHz IEEE 802.15.4 compliant RF Transceiver," http://www.chipcon.com, November 2003.

[16] 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.

[17] P. Levis *et al.*, "The Emergence of Networking Abstractions and Techniques in TinyOS," in *NSDI'04*, 2004.

[18] 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*, 2006.

[19] 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*, 2004, pp. 216–230.

[20] 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: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks.* New York, NY, USA: ACM, 2005, pp. 76–88.

[21] G. Alnifie and R. Simon, "A multi-channel defense against jamming attacks in wireless sensor networks," in *Q2SWinet '07: Proceedings of the 3rd ACM workshop on QoS and security for wireless and mobile networks.* New York, NY, USA: ACM, 2007, pp. 95–104.

[22] A. D. Wood, J. A. Stankovic, and S. H. Son, "JAM: A Jammed-Area Mapping Service for Sensor Networks," in *RTSS*, 2003.

[23] 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 (WiSe)*, 2004, pp. 80–89.

[24] A. Mishra, V. Shrivastava, D. Agrawal, S. Banerjee, and S. Ganguly, "Distributed channel management in uncoordinated wireless environments," in *MobiCom '06*, 2006, pp. 170–181.

[25] 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.

[26] M. Raya, J.-P. Hubaux, and I. Aad, "Domino: a system to detect greedy behavior in ieee 802.11 hotspots," in *MobiSys '04*, 2004, pp. 84–97.

[27] Sherif Khattab, Daniel Mossé, and Rami Melhem. "Jamming mitigation in multi-radio wireless networks: Reactive or proactive?," *under submission*, 2008.

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3604
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3604