Rate Adaptation in Unlicensed Bands under Smart Jamming Attacks

Cankut Orakcal
Dept. of Electrical and Computer Eng.
Boston University
Boston, MA, 02215, USA
Email: orakcal@bu.edu

David Starobinski
Dept. of Electrical and Computer Eng.
Boston University
Boston, MA, 02215, USA
Email: staro@bu.edu

Abstract*—Wireless communication protocols for unlicensed frequency bands support rate adaptation algorithms (RAAs) to cope with time-varying channel conditions. RAAs are not designed to operate against adversarial behavior, however. In this work, we analyze the vulnerabilities of two state-of-the-art RAAs, Minstrel and RARF, against a smart jamming model, whereby an adversary learns the current rate of transmission of each packet before deciding whether to jam the packet or not. Our parameterized analysis, validated by ns-3 simulations, shows that a jamming rate of only 10% is sufficient to bring the throughput of Minstrel below the base rate of 1 Mb/s, whereas RARF requires a jamming rate of 16.7%. These findings are notable since previous work showed that the randomized nature of RARF and Minstrel make them resilient to simpler jamming attacks. The paper concludes by sketching possible solutions to mitigate these sophisticated attacks.

I. Introduction

Nascent cognitive radio technologies promise to make efficient use of temporally or spatially under-utilized frequency bands, e.g., TV white spaces. Similar to 802.11 Wi-Fi devices, cognitive radios cope with time-varying interferences by dynamically adapting radio parameters. Thus, for instance, the Communications Research Centre (CRC) in Canada introduced *CORAL*, a cognitive radio networking platform based on IEEE 802.11a/g standards [1]. CORAL allows users to configure 802.11 parameters such as channel selection, signal strength reporting, acknowledgment policy control and transmit data rate control. This platform enables researchers to investigate novel approaches to broadband wireless networks by using cognitive radio technologies.

In this paper, we are specifically interested in understanding the security implications of rate adaptation on the performance of Wi-Fi networks, as these findings are expected to be relevant to the design of future cognitive radio technologies. The purpose of a rate adaptation algorithm (RAA) is to adapt the transmission rate and the modulation scheme in order to maximize performance (e.g., throughput) based on current wireless channel conditions. The networking community has put great effort on devising efficient RAAs [2]–[6], and several of these algorithms have been commercialized.

Due to the broadcast nature of the wireless channel, security is a major challenge to wireless networks. A major part of attacks against WLANs consists of jamming, which is defined as the obstruction of the wireless medium. Commercial off-the-shelf jamming equipment is easily accessible. For instance, [7] offers easy-to-use and affordable Wi-Fi jammers. Recent studies, such as [8]–[10], show that various jamming attacks described in the literature can be implemented efficiently. A typical jammer aims to cause maximum damage using minimum number of transmissions, in order to avoid being detected and to save energy.

The main motivation behind jamming is to cause Denial of Service (DoS) [11], [12]. Jamming can be used for various purposes, such as personal (deny communication between some parties), economic (competing companies) or governmental (cyber warfare) [13]. Jammers can also perform Reduction of Quality (RoQ) attacks using intelligent jamming patterns [11], [14]. Generally, RoQ attacks exploit vulnerabilities at layers higher than the physical layer. The result is throughput degradation and prolonged delays, which are considered as intolerable in time-critical applications.

RAAs are not designed to operate against adversarial behavior from malicious entities. Many of them fail to distinguish between packet losses due to fluctuations in channel conditions and those due to interference. In other work, we have proposed randomization as a defense mechanism against RoQ attacks employing a periodic jamming model [15]. In this work, we investigate how state-of-the-art RAAs can be exploited using much stronger smart jamming strategies to perform RoQ attacks, even if they employ randomization.

Our contributions in this context are as follows: First, we propose a theoretical framework to formally analyze the vulnerabilities of several existing RAAs to jamming attacks. Specifically, we utilize the *smart jamming* model proposed by Noubir et. al [16], under which an adversary can sniff the Physical Layer Convergence Protocol (PLCP) header [17] of each packet to retrieve the bit-rate used for the transmission of that packet. For this model, we constructively determine strategies and corresponding jamming rates to keep the throughput of RAAs below the base rate (i.e., the lowest bit-rate). For default parameters, we show that low jamming rates of about 10% for the state-of-the-art Minstrel algorithm, and 16.7%

This work was supported in part by the U.S. National Science Foundation under grants CNS-1012910 and CCF-0916892.

for RARF (a randomized algorithm that we have proposed in [15]) are sufficient to achieve this goal. Our analysis also provides expressions for general parameter settings. Based on our analysis, we highlight a trade-off between exploiting a well performing rate and probing potentially better rates. Finally, we conduct ns-3 simulations implementing various RAAs and jamming strategies for an IEEE 802.11g WLAN. Our simulations validate the jamming strategies under different channel models.Finally, we sketch possible solutions to avoid or mitigate smart jamming attacks. Note that detailed pseudocodes of Minstrel and RARF can be found in [18].

The rest of this paper is organized as follows. In Section II, we review related work. Next, we introduce our theoretical model in Section III. Then, we analyze the impact of smart jamming on Minstrel and RARF in Section IV. Finally, we present the results of our ns-3 simulations in Section V and conclude the paper in Section VI.

II. Related Work

In this section, we provide necessary background through a survey of the related work in the literature. The majority of the related work can be broadly classified into three categories; those which study the performance of RAAs under heavy congestion, those which experimentally demonstrate the vulnerabilities of RAAs against jamming, and those which study rate control mechanisms in 802.11n networks.

The purpose of an RAA is to adaptively pick the best possible rate, based on changing wireless channel conditions. Various approaches have been proposed for rate control in IEEE 802.11 WLANs. Transmission rate can be adjusted by estimating the channel conditions using packet losses [2]–[4], [15], [19], [20], Signal to Interference and Noise Ratio (SINR) measurements [21], [22], or throughput estimates [5], [6].

Many proposed RAAs fail to distinguish packet losses due to channel conditions from those due to interference. The vulnerability of RAAs to interference has been studied in the literature and some countermeasures have been proposed. Chen et al. [23] investigate the performance of RAAs in heavily congested wireless networks, where most of the packet losses are due to interference from neighboring cells. Employing RAAs in such an environment decreases the transmission rate due to high packet loss probabilities, resulting in longer transmission times. In turn, such longer transmissions further increase the packet loss ratio, thus causing a positive feedback. To overcome this effect, the authors of [23] propose a *Rate Adaptive Framing* mechanism for highly interfered networks. This mechanism, however, applies to non-malicious interferences caused by other network nodes, rather than those caused by an adversary.

To our knowledge, the work of Pelechrinis et al. [24] is the first to study the effect of jamming on the RAA performance. The authors employ a random jamming model that alternates between jamming and idle periods that are uniformly distributed. They demonstrate that, for several widely deployed RAAs, throughput reduces drastically under select jamming attacks, whereas fixed rate transmission provides higher throughput. Thus, this work proposes an anti-jamming scheme called *ARES* that uses rate adaptation when the jammer is idle, and uses fixed rate transmission otherwise. *ARES* adjusts the carrier sense threshold, so that packets can be received even when a jammer is actively transmitting. This scheme assumes that there exists a perfect jamming detection mechanism, which is a non-trivial problem. Moreover, adjusting the carrier sense threshold under jamming works only if the transmission power of the jammer is lower than of non-malicious nodes, which is an assumption that might not always hold.

The recent work of Noubir et al. [16] investigates the vulnerability of several RAAs against smart (selective) jamming attacks. The authors show the existence of effective attacks to degrade system performance. A jammer sniffs the header of each packet to retrieve the bit-rate used for the transmission of that packet. Based on this rate information, the jammer instantly decides whether to jam the packet or not. In this work, we utilize the same model. However, in contrast to our paper, the work in [16] does not explicitly analyze the performance of each RAA under jamming.

In other work [15], we have analyzed the vulnerabilities of deterministic RAAs to periodic jamming attacks and proposed judicious use of randomization to address this problem. However in this work, we consider smart jamming model (which is much stronger than periodic jamming) and demonstrate that randomization, as employed in RARF and Minstrel, is not an effective means for robust rate control under smart jamming.

Although the work we have considered until now is related to 802.11a/b/g standards, rate control in 802.11n networks has also been studied. Kim et. al [25] and Lakshmanan et. al [26] experimentally demonstrate that trivial extensions of existing rate control algorithms do not perform well for 802.11n, due to the growth in degrees of freedom, including not only the modulation and coding scheme but also the number of spatial streams and the specific antenna elements. Perfianakis et. al [27] discover a non-monotonic relation between packet loss and transmission rate in 802.11n MIMO scenarios and propose *MiRa*, a MIMO rate control scheme that zigzags between single stream and double stream modes using extensive probing. Finally, Peng et. al [28] and Xi et. al [29] propose MIMO rate adaptation algorithms that require physical layer feedback from the receiver, which is allowed in 802.11n [30], and include strong assumptions about the channel model.

To our knowledge, none of the RAAs designed specifically for 802.11n have been implemented on commercial off-the-shelf equipment yet [31], [32]. Thus, the jamming strategies that we consider in this work can be applied to MIMO systems that implement extensions of 802.11g RAAs. Furthermore, prior work on 802.11n WLANs does not address the security issues related to RAAs. Jamming resistance is not considered in the design of new RAAs for 802.11n.

III. Models and Notation

A. Channel Model

We assume that n possible transmission rates exist, denoted by $R_1, R_2, \ldots, R_n$, where $R_1 < R_2 < \ldots < R_n$. For instance, IEEE 802.11g standard allows transmission at $n = 12$ different bit-rates. For each RAA that we analyze, we first assume a perfect channel model (i.e., packet loss is only due to jamming) and then extend the analysis to non-perfect channel conditions (i.e., packet loss is due either to jamming or to non-malicious interferences).

Let α_i denote the long run proportion of packets transmitted at the bit-rate R_i. The long run proportion of packet losses at the bit-rate R_i in the presence of a jammer is denoted f_i. We define *steady-state throughput* as:

$$Thr = \sum_{i=1}^{n} \alpha_i \left(1 - f_i\right) R_i. \tag{1}$$

To keep the analysis tractable, we ignore all control packets, back-off retransmissions, and inter-frame spacings while calculating the steady state throughput. Note that our definition of throughput corresponds to the average transmission rate per packet, and therefore avoids the need to make any assumptions about the length of each packet.

B. Jamming Model

In this paper, we consider a *smart jamming* model, introduced by [16]. Under this model, a jammer is capable of sniffing the PLCP header of each packet to retrieve the bit-rate used for the transmission of that packet. Based on this rate information, the jammer instantly decides whether to jam that packet or not. A jammed packet is corrupted and lost.

The *Rate of Jamming*, abbreviated RoJ, is the main metric of interest in this paper. It is defined as the ratio of number of jammed packets to the total number of transmitted packets. For each RAA studied in this paper, our goal is to find the minimum value of RoJ (or a bound on it) to keep the throughput of the RAA below the base rate R_1. For 802.11g, this corresponds to a 98% degradation in throughput under perfect channel conditions. Although the aim of the jammer is highly aggressive, we will demonstrate that it can be achieved with low RoJ values. A low RoJ implies that an RAA is highly vulnerable to jamming attacks, while a high RoJ implies that the RAA is resilient.

According to [11], a feasible jamming attack should have the following properties:

- High energy efficiency,
- Low detection probability,
- High levels of DoS,
- Resistance to physical layer anti-jamming techniques.

In order to avoid detection, the jammer can employ RoQ attacks, which reduce the system performance by applying only a limited jamming rate [14]. The low volume of the RoQ attack makes it difficult to effectively identify the attack. In addition, packet losses due to wireless channel conditions and interferences further decrease the possibility of detection. Thus, minimizing RoJ value provides both efficiency and low probability of detection.

IV. Analysis of RAAs under Jamming

In this section, we provide constructive bounds on the jamming rates required to keep the throughput of Minstrel and RARF below the lowest possible bit-rate. First, we assume a perfect channel model and two bit-rates (R_1 and R_2) for the sake of tractability. Later, we generalize our discussion to non-perfect channels and any set of bit-rates. We also assume that each RAA starts from R_1, due to an initial jamming phase. In the following, RoJ_{RAA} denotes the jamming rate required to keep the throughput of the RAA scheme below R_1 and Thr_{RAA} denotes the resulting throughput.

A. Minstrel

Minstrel is widely deployed in commercial off-the-shelf equipment [6]. Although the operation of Minstrel is complex, it can be summarized in a few steps.

First of all, Minstrel involves periodic updates. The default value of an update window is 100 ms. Within each update window, Minstrel sends probe packets at random bit-rates (called a sampled rate). A probe packet is sent with probability 0.5 if the ratio of the number of probe packets to the number of all packets is lower than 10%. Secondly, Minstrel involves multi-rate retries, i.e. if a packet transmission fails; transmission is retried using different bit-rates. For instance, if the sampled rate is higher than the current rate, then the probe packet is sent immediately. Otherwise, the sampled rate is tried only if the current transmission fails. The exact structure of the retry chain for probe packets and data packets differ as detailed in [18]. Based on the transmission results of the probe packets, Minstrel calculates a throughput estimate for each bit-rate attempted. Using the throughput estimates, Minstrel picks the bit-rate with the highest throughput at the end of an update window and uses that rate for the upcoming update window (except for probe packets).

Minstrel is implemented using two subroutines: $updateStats()$ and $findRate()$. The $updateStats()$ subroutine calculates the throughput estimates for each attempted bit-rate based on transmission results, whereas the $findRate()$ subroutine selects which rates to use for data packets and probe packets, and when to send probe packets. Detailed pseudo-codes are given in [18].

An effective smart jamming strategy against Minstrel is to jam all probe packets that are transmitted at R_2. This way, the system cannot switch to R_2 and the throughput is kept below R_1. The jamming rate and the resulting throughput value of this strategy are calculated in the proof of Theorem 1.

Theorem 1. *The throughput of two-rate Minstrel can be kept below R_1 by using a smart jammer with jamming rate:*

$$RoJ_{\text{Minstrel}} = 10\%,$$

for all parameter values.

Proof: This jamming strategy requires the jammer to destroy any packet transmitted at R_2. Since we assume that Minstrel is initiated from R_1, any such packet is a probe packet. If all probe packets are successfully jammed, the throughput estimate at R_2 will be zero and the system will be stuck at R_1. The jamming rate is equal to the percentage of probe packets in the long run. Note that this percentage is always equal to 10%, regardless of parameter values. The resulting values are:

- $\alpha_1 = 0.9\,, \alpha_2 = 0.1\,,$
- $f_1 = 0,\ f_2 = 1\,.$

Using Eq. (1), we calculate the resulting throughput as $Thr_{\text{Minstrel}} = 0.9R_1$. ■

This strategy works for any set of bit-rates and under any channel conditions due to the ability of the jammer to receive feedback. In fact, any packet loss caused by the channel might result in an even lower RoJ value.

B. RARF

Randomized Automatic Rate Fallback (RARF) is a randomized variant of ARF, which is the first documented RAA. In [15], we have shown that deterministic RAAs are highly vulnerable against simple periodic jamming attacks. Thus, we have proposed RARF as a means to improve the resistance of RAAs to periodic jamming attacks. Basically, RARF switches to the next higher rate (if possible) after each successful packet transmission with probability s^{-1}. Furthermore, it switches to the next lower rate (if possible) after f consecutive packet transmission failures.

Next, we analyze the behavior of RARF under smart jamming. The strategy is to destroy all packets that are transmitted at rates higher than R_1. The jamming rate and the resulting throughput value are calculated in the proof of Theorem 2.

Theorem 2. *The throughput of two-rate RARF can be kept below R_1 by using a smart jammer with jamming rate:*

$$RoJ_{\text{RARF}} = \frac{f}{s+f}\ .$$

For default parameter values (i.e., $s = 10$ and $f = 2$), $RoJ_{\text{RARF}} \approx 16.7\%$.

Proof: This jamming strategy requires the jammer to destroy any packet that is transmitted at R_2. When RARF switches to R_2, the jammer starts destroying packets until the system goes back to R_1. Since RARF requires f consecutive failures to pick the next lower rate, the jammer should destroy f packets when it is active.

After each active period, RARF is guaranteed to transmit at R_1. The number of packets transmitted at R_1 has a geometric distribution with parameter s^{-1}. The expected value of this distribution is equal to s and the jammer is idle during these transmissions. Thus, idle and active periods of the jammer add up to $s + f$ in expectation. The resulting values are:

- $\alpha_1 = s\,(s+f)^{-1},\ \alpha_2 = RoJ_{\text{RARF}} = f\,(s+f)^{-1},$
- $f_1 = 0,\ f_2 = 1.$

Using Eq. (1), we calculate the resulting expected throughput as $Thr_{\text{RARF}} = s\,(s+f)^{-1}R_1$. ■

This strategy works for any set of bit-rates since the jammer does not allow the system to transmit even at R_2. It also works for any channel conditions, and packet losses caused by the channel might result in an even lower RoJ value.

C. Discussion of Analytical Results

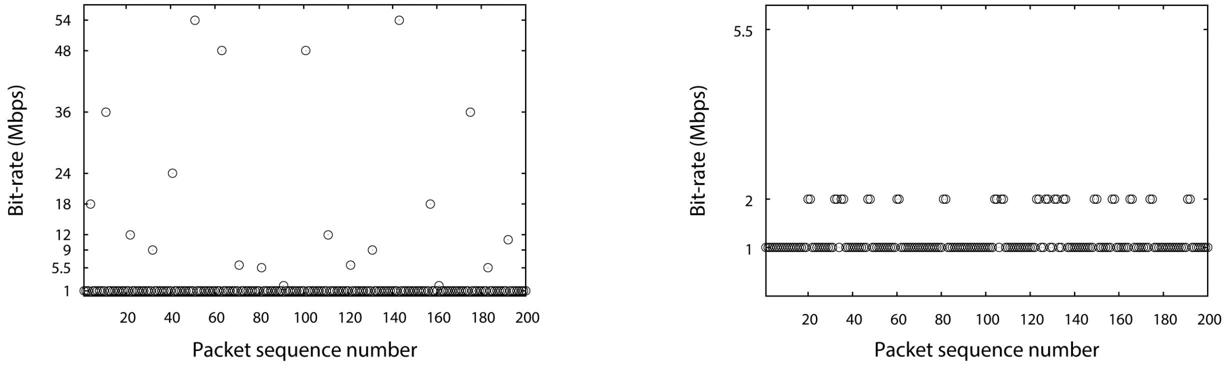
In our analysis, we have assumed that both RAAs start from R_1 due to an initial jamming phase. If the system does not start the transmission at R_1, deriving an initial jamming strategy is a simple task and does not alter the steady-state pattern of the jammer. For instance, the initial jamming phase for Minstrel shouldcause the throughput estimates of all rates higher than R_1 to be lower than the estimate of R_1. For RARF, jamming $(n-1)f$ consecutive packets guarantees that the system to go down to R_1. Since we consider the steady state behavior, these initial phases can be ignored in the calculation of RoJ.

For both Minstrel and RARF, although a lower RoJ value might be enough under lossy channel conditions, the jammer should always utilize the strategy employed for the perfect channel to make sure that the throughput is lower than R_1. In this work, we discuss jamming strategies that work no matter what the channel characteristics are. According to our model, the jammer does need to have any knowledge about the success of packet transmissions. Obviously, such knowledge could only further help the jammer in further reducing its jamming rate.

For default parameter values, we observe that RARF is more resilient against smart jamming attacks than Minstrel. However, this is due to a typical trade-off in rate control. If an RAA heavily exploits a bit-rate and rarely probes other rates, then it generally performs well under stable conditions but becomes less responsive to sudden changes in the channel. Such an algorithm might also be vulnerable to simple jamming attacks since destroying a few probes can be done efficiently. On the other hand, if an RAA is designed to probe other rates more frequently, then dynamic channels are estimated more accurately but many probe packets might be wasted under a stable channel. Such an approach has higher jamming resistance due to the large number of probe packets to be destroyed. Nevertheless, one should keep in mind that jamming resistance is not the main purpose of an RAA. Typically, parameters of RAAs are set based on extensive experimental studies.

D. Mitigations

Several defense mechanisms against smart jamming attacks might be possible. A trivial solution is to use encrypted PLCP headers in order to prevent the jammer to retrieve the real time transmission rate, as suggested in [16]. However, this approach requires the encryption and decryption of the PLCP header for each packet, which introduce a large overhead and high computational complexity. Secondly, network nodes could utilize *closed loop* rate adaptation, which allows the transmitter to receive feedback from the receiver, as supported in 802.11n [30]. By sending predetermined signal patterns, nodes can estimate the channel and adapt the rate accordingly, without considering individual packet losses. Lastly, the smart jamming strategies that we have considered are fairly aggressive. Thus, if certain rates consistently perform poorly,



(a)

(b)

Fig. 1: Performance under perfect channel with smart jamming. Each data point indicates a packet transmission. (a) Minstrel under jamming with $RoJ = 10.1\%$. $Thr = 0.899$ Mb/s ; (b) RARF under jamming with $RoJ = 16.6\%$. $Thr = 0.834$ Mb/s.

a signature-based detection or anomaly detection mechanism could be triggered.

V. Simulation Results

In this section, we present the results of ns-3 [33] simulations of IEEE 802.11g WLANs to validate our analytical findings. The goals of our simulations are to monitor the bit-rate used for each packet and to measure the steady state throughput of a system that employs a specific RAA under a given jamming strategy.

A. Set-up

We use standard ns-3 libraries whenever possible. We have built a new ns-3 module for RARF, since it is not available in the standard library. In all of our simulations, we assume that the length of each DATA packet is 1250 bytes. We use IEEE 802.11g in its ad-hoc mode since we consider two stations and wish to avoid beacons. The jammer is implemented by modifying `ns3::YansWifiPhy` class, which implements the physical layer of IEEE 802.11. `JAMMED` flag is added to each packet, with default value 0. The transmitter checks the bit-rate used for each packet and whenever a packet is transmitted at a rate higher than 1 Mb/s, the transmitter sets the `JAMMED` flag to 1. When the receiver gets a packet with `JAMMED` flag 1, it treats the packet as lost, and does not send an acknowledgement. Note that acknowledgements are not jammed. Although our ns-3 simulations take control packets, back-off retransmissions, and inter-frame spacings into consideration, the resulting throughput values are based on our definition in Section III-A.

B. Perfect Channel

We test the performance of Minstrel and RARF under smart jamming as in Fig. 1. Each data point indicates a DATA packet transmission. Simulations are run for 100 seconds assuming perfect channel conditions. Fig. 1(a) illustrates the result of the jamming strategy given by Theorem 1 on Minstrel. The smart jammer is able to destroy all probe packets at high bit-rates by using a jamming rate of 10.1%. We also apply smart jamming on RARF as in Fig. 1(b). In this case, required RoJ value is around 16.6%. This result demonstrates that for default parameter values, RARF is slightly more resilient than Minstrel under a stronger jamming model.

C. Lossy Channel

In this section, we perform simulations using the `ns3::LogDistancePropagationLossModel` of ns-3. This model has the following parameters:

- n : the path loss distance exponent
- d_0 : reference distance (m)
- L_0 : path loss at reference distance (dB)
- d : distance (m)
- L : path loss (dB)

The reception power is calculated using the log-distance propagation loss model in the following way:

$$L = L_0 + 10\, n\, \log_{10}\left(\frac{d}{d_0}\right). \qquad (2)$$

The default parameter values for this channel model are $n = 3$, $d_0 = 1\ m$, and $L_0 = 46.677\ dB$. Under this channel model, we have implemented the corresponding effective jamming strategies for each RAA with $d \in \{10, 20, \ldots, 200\}\ m$, $n \in \{1, 2, \ldots, 5\}$, and default values for d_0 and L_0. For both Minstrel and RARF, the jamming strategies again manage to keep the throughput below 1 Mb/s. The results for $d = 100\ m$ and $n = 3$ are given in Table I.

TABLE I: Throughput values of Minstrel and RARF with corresponding effective jamming strategies under a lossy channel. The strategies still manage to keep the throughput below R_1.

RAA	**Jamming Rate**	**Thr**
Minstrel	$RoJ = 10.0\%$	0.900 Mb/s
RARF	$RoJ = 16.1\%$	0.839 Mb/s

VI. Conclusion and Future Work

In this work, we analyzed the vulnerabilities of rate control mechanisms against smart jamming patterns and corroborated our results using network simulations. Our contributions in this work can be listed as follows: First, we introduced a theoretical framework that employs a smart jamming model and a rate of jamming metric to analyze the vulnerabilities of RAAs in unlicensed wireless networks. In our analysis, we proved that the jamming rate required to keep throughput performance below the base rate is low for Minstrel (around 10%), and slightly higher for RARF (around 16.7%). The difference is mainly due to default parameter values. These results enabled us to observe the trade-off between exploiting a well performing rate and probing potentially better rates. We corroborated our analytical results using ns-3 simulations. Our simulations revealed that the same jamming strategies can be employed for both perfect and lossy channels.

In summary, our analytical findings and ns-3 simulations show that state-of-the-art RAAs are vulnerable to selective jamming attacks. We have observed that although randomization is an effective defense mechanism against periodic jamming attacks, it does not provide robustness against stronger jamming models such as smart jamming. That said, we sketched possible solutions for mitigating this problem. Further work is needed to thoroughly evaluate these solutions.

References

[1] CRC Canada, "CORAL - Cognitive radio learning platform," http://www.crc.gc.ca/files/crc/home/wifi_cr/coral_brochure_en.pdf.

[2] A. Kamerman and L. Monteban, "WaveLAN: A high-performance wireless LAN for the unlicensed band," *Bell Labs Technical Journal*, vol. 2, no. 3, pp. 118–133, 1997.

[3] M. Lacage, M. H. Manshaei, and T. Turletti, "IEEE 802.11 rate adaptation: a practical approach," in *MSWiM*, Venice, Italy, 2004.

[4] Onoe, "MadWifi rate control," http://madwifi-project.org/browser/madwifi/trunk/ath_rate/onoe, 2011.

[5] J. C. Bicket, "Bit-rate selection in wireless networks," Master's thesis, Massachusetts Intitute of Technology, 2005.

[6] Minstrel, "MadWifi rate control," http://madwifi-project.org/browser/madwifi/trunk/ath_rate/minstrel, 2011.

[7] Jammer-Store, "Portable Wi-Fi jammers, powerful bluetooth Wi-Fi signal jammers for sale," http://www.jammer-store.com/, 2012.

[8] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short paper: reactive jamming in wireless networks: how realistic is the threat?" in *WiSec*, Hamburg, Germany, 2011.

[9] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *MOBIHOC*, Urbana-Champaign, IL, USA, 2005.

[10] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan, "Understanding and mitigating the impact of RF interference on 802.11 networks," in *SIGCOMM*, Kyoto, Japan, 2007.

[11] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *Communications Surveys & Tutorials, IEEE*, vol. 13, no. 2, pp. 245–257, 2011.

[12] B. Zhou, A. Marshall, W. Zhou, and K. Yang, "A random packet destruction DoS attack for wireless networks," in *ICC*, Beijing, China, 2008.

[13] A. Scott, T. Hardy, R. Martin, and R. Thomas, "What are the roles of electronic and cyber warfare in cognitive radio security?" in *MWSCAS*, Seoul, Korea, 2011.

[14] W. Chen, Y. Zhang, and Y. Wei, "The feasibility of launching reduction of quality (RoQ) attacks in 802.11 wireless networks," in *ICPADS*, Melbourne, Victoria, Australia, 2008.

[15] C. Orakcal and D. Starobinski, "Jamming-resistant rate control in IEEE 802.11 WLANs," Boston University, CISE Technical Report (submitted for conference publication) 2011-IR-0021, 2011, also available as http://www.bu.edu/phpbin/cise/download.php?publication_id=1129.

[16] G. Noubir, R. Rajaraman, B. Sheng, and B. Thapa, "On the robustness of IEEE802.11 rate adaptation algorithms against smart jamming," in *WiSec*, Hamburg, Germany, 2011.

[17] D. Coleman, D. Westcott, B. Miller, and P. Mackenzie, *CWAP Certified Wireless Analysis Professional Official Study Guide: Exam PW0-270*, ser. CWNP Official Study Guides. John Wiley & Sons, 2011.

[18] C. Orakcal, "Jamming-resistant rate control in Wi-Fi networks," Master's thesis, Boston University, 2012.

[19] S. Wong, H. Yang, S. Lu, and V. Bharghavan, "Robust rate adaptation for 802.11 wireless networks," in *MobiCom*, Los Angeles, CA, USA, 2006.

[20] J. Kim, S. Kim, S. Choi, and D. Qiao, "CARA: Collision-aware rate adaptation for IEEE 802.11 WLANs," in *INFOCOM*, Barcelona, Spain, 2006.

[21] G. Holland, N. Vaidya, and P. Bahl, "A rate-adaptive MAC protocol for multi-hop wireless networks," in *MobiCom*, Rome, Italy, 2001.

[22] M. Vutukuru, H. Balakrishnan, and K. Jamieson, "Cross-layer wireless bit rate adaptation," in *SIGCOMM*, Barcelona, Spain, August 2009.

[23] C. Chen, H. Luo, E. Seo, N. H. Vaidya, and X. Wang, "Rate-adaptive framing for interfered wireless networks," in *INFOCOM*, Anchorage, Alaska, USA, 2007.

[24] K. Pelechrinis, I. Broustis, S. V. Krishnamurthy, and C. Gkantsidis, "ARES: An anti-jamming reinforcement system for 802.11 networks," in *CoNEXT*, Rome, Italy, 2009.

[25] W. Kim, O. Khan, K. Truong, S. Choi, R. Grant, H. Wright, K. Mandke, R. Daniels, R. Heath, and S. Nettles, "An experimental evaluation of rate adaptation for multi-antenna systems," in *INFOCOM*, Rio de Janeiro, Brazil, 2009.

[26] S. Lakshmanan, S. Sanadhya, and R. Sivakumar, "On link rate adaptation in 802.11n WLANs," in *INFOCOM*, Shanghai, China, 2011.

[27] I. Pefkianakis, Y. Hu, S. Wong, H. Yang, and S. Lu, "MIMO rate adaptation in 802.11n wireless networks," in *MobiCom*, Chicago, Illinois, USA, 2010.

[28] F. Peng, J. Zhang, and W. Ryan, "Adaptive modulation and coding for IEEE 802.11n," in *WCNC*, Hong Kong, 2007.

[29] W. H. Xi, A. Munro, and M. Barton, "Link adaptation algorithm for the IEEE 802.11n MIMO system," in *NETWORKING*, Singapore, 2008.

[30] S. Abraham, A. Meylan, and S. Nanda, "802.11n MAC design and system performance," in *ICC*, Seoul, Korea, 2005.

[31] MadWifi-Project, "Bit-rate selection algorithms," http://madwifi-project.org/wiki/UserDocs/RateControl, 2012.

[32] LinuxWireless, "mac802.11 rate control algorithms," http://linuxwireless.org/en/developers/Documentation/mac80211, 2012.

[33] ns 3, "Network simulator," http://www.nsnam.org/, 2012.