Jamming-Resistant Rate Adaptation in Wi-Fi Networks[☆]

Cankut Orakcal[a,*], David Starobinski[a]

[a] *Boston University, Dept. of Electrical and Computer Eng., Boston, MA, USA 02215*

Abstract

We introduce a theoretical framework to formally analyze the vulnerability of IEEE 802.11 rate adaptation algorithms (RAAs) to selective jamming attacks, and to develop countermeasures providing provable performance guarantees. Thus, we propose a new metric called Rate of Jamming (*RoJ*), wherein a low *RoJ* implies that an RAA is highly vulnerable to jamming attacks, while a high *RoJ* implies that the RAA is resilient. We prove that several state-of-the-art RAAs, such as ARF and SampleRate, have a low *RoJ* (i.e., 10% or lower). Next, we propose a robust RAA, called Randomized ARF (RARF). Using tools from renewal theory, we derive a closed-form lower bound on the *RoJ* of RARF. We validate our theoretical analysis using ns-3 simulations and show that the minimum jamming rate required against RARF is about 33% (i.e., at least three times higher than the *RoJ* of other RAAs).

Keywords: IEEE 802.11, Denial of Service, rate control.

1. Introduction

Wireless local area networks (WLANs), based on the IEEE 802.11 (Wi-Fi) family of standards, play a major role in the current Internet infrastructure. According to [1], over 100,000 public Wi-Fi hotspots have been deployed

[☆] A shorter version of this paper appeared in the proceedings of IEEE GLOBECOM 2012.

[*] Corresponding author, Tel: +1 857 654 0018

Email addresses: orakcal@bu.edu (Cankut Orakcal), staro@bu.edu (David Starobinski)

in the U.S. Furthermore, several cellular network providers, such as AT&T, are deploying Wi-Fi hotspots to offload congestion in crowded areas (e.g., stadiums) [2].

IEEE 802.11 supports data transmission at multiple bit-rates. Several *rate adaptation algorithms* (RAAs), also known as *rate control mechanisms*, have been proposed 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 proposing efficient RAAs [3, 4, 5, 6, 7], and several of these algorithms have been commercialized.

Security has always been challenge to wireless services due to the broadcast nature of the wireless channel. A major part of attacks against Wi-Fi consists of jamming, i.e., obstruction of the wireless medium. Commercial off-the-shelf jamming equipment is at reach of anyone's hands, and makes such attacks easy to launch. For instance, [8] offers affordable Wi-Fi jammers that are activated by a single button. Recent studies [9, 10, 11] reveal that various jamming attacks described in the literature can be implemented efficiently. Typically, a jammer aims to cause maximum damage using a minimum number of transmissions to avoid getting detected and to save energy.

The main motivation behind jamming is to cause *Denial of Service* (DoS) [12, 13]. Jamming can be used for personal purposes (deny communication between some parties), economic purposes (competing companies) or governmental purposes (cyber warfare) [14]. However, causing complete DoS generally requires jamming all data exchanges between two parties. For this purpose, a jammer should destroy each data packet or corresponding acknowledgment packet.

Reduction of Quality (RoQ) attacks can also be performed using intelligent jamming patterns [12, 15, 16]. Typically, RoQ attacks exploit vulnerabilities above the physical layer. The result is degradation of throughput and prolonged delays, which significantly affect the quality of service perceived by users.

Rate control mechanisms are not designed to operate against adversarial behavior from malicious entities. Most RAAs cannot distinguish between packet losses due to fluctuations in channel conditions and those due to interference. Thus, recent experimental studies [17, 18] demonstrate that several well-known and widely deployed rate adaptation algorithms used in 802.11 WLANs are vulnerable to jamming attacks (cf. Section 2 for a detailed discussion). However, these works are either based on different jamming

models [18] or do not present solutions with theoretical guarantees [17].

In this paper, we investigate the vulnerabilities of state-of-the-art RAAs to RoQ attacks. We develop a mathematical approach to derive jamming strategies that are effective for *general* parameter settings. For 802.11g networks, we show that causing 98% throughput degradation can be achieved by very efficient jamming attacks. Our contributions in this context are as follows:

- We introduce a theoretical framework to formally analyze the vulnerabilities of several existing RAAs to jamming attacks, using a performance metric called Rate of Jamming (RoJ). The framework is based on a jamming model, called *bursty periodic jamming*, under which an adversary periodically jams the channel with a burst of packets.

- 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 parameter values, we derive low jamming rates of about 9% for the early ARF algorithm and 4% for the newer SampleRate algorithm are sufficient to achieve this goal.

- We propose a new algorithm, called Randomized ARF (RARF), as a means to improve the resistance of RAAs to jamming attacks. We analytically show that RARF performs *comparably* to ARF under *no jamming*, but performs *much better under targeted jamming attacks* due to its randomized nature. We derive a closed-form lower bound on the minimum RoJ required to keep the throughput of a system that employs RARF below the base rate. For default parameters, this value is about 20%.

- 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, demonstrating that they indeed bring the throughput of the studied RAAs close to the base rate. Furthermore, the simulation results reveal that the RoJ of RARF is about 33% in practice (i.e., at least three times higher than the RoJ of other RAAs).

We stress that the main contributions of this paper are to derive close-form analytical results on the performance of RAAs under smart jamming

attacks and come up with a solution providing theoretical guarantees. We do not provide experiments on a real testbed, since earlier work already demonstrates existence of efficient jamming attacks, including smart ones, on RAAs through experimentation [17, 18, 19].

The rest of this paper is organized as follows. In Section 2, we review related work. Next, we introduce our theoretical model in Section 3 and analyze the impact of bursty periodic jamming on several RAAs in Section 4. Then, we propose and analyze a new randomized jamming-resistant approach in Section 5. We present our ns-3 simulation results in Section 6 and conclude the paper in Section 7. Due to space limitations, pseudo-codes of RAAs are deferred to [20].

2. Related Work

In this section, we provide necessary background through a survey of the related work in the literature. First, we discuss several approaches in rate control schemes. Then, we review the related work in two main categories; those which study the performance of RAAs under heavy congestion, and those which experimentally demonstrate the vulnerabilities of RAAs against jamming.

2.1. Approaches in Rate Control

The purpose of an RAA is to adaptively pick the best possible transmission 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 [4, 5, 7, 21, 22], Signal to Interference and Noise Ratio (SINR) measurements [23, 24], or throughput estimates [3, 6].

Notable RAAs employed in 802.11a/b/g systems include ARF [4], AARF [5], Onoe [7], SampleRate [3] and Minstrel [6], all of which have been used in commercial off-the-shelf equipment [25, 26]. Some of these algorithms are described in detail when their performances are analyzed in Section 4.

Rate control in 802.11n networks has also been studied. Pefkianakis et al. [27] discover a non-monotonic relation between packet loss ratio and transmission rate in 802.11n MIMO scenarios, and propose a MIMO rate control scheme called *MiRa* that zigzags between single stream and double stream modes using extensive probing. Peng et al. [28] and Xi et al. [29] propose MIMO rate adaptation algorithms that estimate and predict the channel for

each packet, calculate the modulation and coding scheme (MCS) that gives the best performance at the receiver side, and send the optimum MCS back to the sender to be used in subsequent transmissions. Both systems require physical layer feedback from the receiver, which is allowed in 802.11n [30], but include strong assumptions about the channel. To our knowledge, none of the RAAs designed specifically for 802.11n systems have been implemented on commercial off-the-shelf equipment yet [25, 26].

2.2. RAAs Under Congestion

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. [31] 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 causes the transmission rate to decrease 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 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 a jammer.

Sheth et al. [32] design and implement mechanisms that can distinguish between different causes of wireless anomalies at the physical layer. The authors demonstrate that using rate fallback in the presence of excessive noise in the channel does not remedy the problem. Thus, they propose a scheme, called *MOJO*, that switches to a less noisy channel when a rise in the noise level is detected, instead of using rate adaptation. Although this defense mechanism might be effective under congestion scenarios, an adversary might have the capability to switch wireless channels as well.

2.3. RAAs Under Jamming

Broustis et al. [19] investigate jamming attacks that exploit medium access protocols in 802.11. The authors demonstrate that attacking a single node degrades the entire WLAN performance due to a performance anomaly caused by rate adaptation. They propose *FIJI*, a defense mechanism to identify the node under attack and prevent the other nodes to be affected

by using transmission delay measurements. In our work, we analyze RoQ attacks that directly target RAAs rather than MAC protocols, and propose a defense mechanism that improve the resiliency of nodes under attack.

To our knowledge, Pelechrinis et al. [18] are the first to study the effect of jamming on the performance of RAAs. This work employs a random jammer that alternates between jamming and idle periods that are uniformly distributed. It demonstrates that, for several popular RAAs, system performance reduces drastically under select jamming attacks, whereas fixed rate transmission provides higher throughput. Thus, the authors propose 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 in order to avoid performing carrier sensing and backoff for specific ranges of observed RSSI, so that packets can be received even when a jammer transmits. The work of *ARES* is based on an intermittent jamming model whereby the attacker jams during (random) periods of time that are sufficiently long to allow detection of the jammer. In contrast, our paper considers a reactive jamming model, whereby the attacker emits bursts energy over short periods of time.

The work of Fragkiadakis et al. [33] provides lightweight intrusion detection mechanisms for wireless networks, for a network using a fixed bit rate. In multi-rate scenarios, where packet losses may be due to transmissions at high bit rates, a detection algorithm that associates a rise in packet loss ratio with the presence of a jammer might not be effective.

The recent work of Noubir et al. [17] investigates the vulnerability of several RAAs against smart (reactive) jamming attacks, and shows the existence of effective attacks to degrade system performance. A jammer sniffs 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 the packet or not. In contrast to our work, the work in [17] does not explicitly analyze the performance of each RAA under jamming. There is no explicit construction for the jammer model and the authors do not provide a feasible and tested solution to address the vulnerability of RAAs to jamming. While randomization is mentioned as a possible solution in [17], no concrete algorithm or analysis is presented. An important contribution of our paper is to devise such an algorithm and carefully analyze its properties. Furthermore, the need of interpreting packet information for every transmission has high computational complexity. In our work, we show that such a complex jammer is unnecessary to significantly degrade the

performance of WLANs. Since many RAAs are deterministic, an adversary knows how an RAA behaves without having to retrieve the bit-rate used for each packet. Additionally, the work of [17] constructs a jamming attack against SampleRate such that about 10% of the packet transmissions need to be jammed in order to keep it at the base-rate. In Section 4, we propose a jamming attack against SampleRate with a jamming ratio smaller than 5%.

In this paper, we analyze the vulnerabilities of deterministic RAAs to periodic jamming attacks and propose judicious use of randomization to address this problem. In other work [34], we consider the effects of more capable jamming models on randomized RAAs, and investigate the robustness of randomization as a defense mechanism.

3. System Model

3.1. Channel Model

We assume that there exists n possible transmission rates denoted as $R_1, R_2, \ldots, R_n$, where $R_1 < R_2 < \ldots < R_n$. For instance, IEEE 802.11g standard allows transmission at $n = 12$ different bit-rates. Let α_i denote the long run proportion of packets transmitted at the bit-rate R_i, and ϕ_i denote the long run proportion of packet losses at the bit-rate R_i in the presence of a jammer. We define *steady-state throughput* as:

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

Note that in Eq. (1) we ignore all control packets, time between backoff retransmissions, and inter-frame spacings. Thus, our definition of throughput corresponds to the average rate used per packet transmission.

3.2. Jamming Model

In this paper, we consider a *bursty periodic* jamming model. Practical implementation of a similar jamming model is demonstrated by Bayraktaroglu et al.[35]. Under such a model, a jammer is capable of jamming a consecutive packets out of every T packets (note that periodicity is defined here with respect to packets, not time). We refer to T as the *jamming period* and to a as the *jamming burst size*. The value of a can be any positive integer, and T must always be greater than a. This model is a special case of the (T, λ)

model introduced in the work of Awerbuch et al. [36] and a form of *shrew attack* [16].

The jammer requires no knowledge of the real-time transmission rate or the history of rates used. The only information available to the jammer is the RAA implemented on the target system. Note that some algorithms used in commercial hardware are available online (e.g., MadWifi Atheros chipsets [25, 26]). In particular, the pseudo-code of the ARF and Sample-Rate algorithms analyzed in our paper are publicly known. While other rate control mechanisms may be unknown, they could be reverse engineered.

The jammer is reactive, i.e., it employs carrier sensing in order to jam the channel only if there is an ongoing packet transmission. Note that a reactive jammer exploits the fact that the emission of a small amount of energy is sufficient to cause packet drops at the legitimate receiver [10, 35].

The *Rate of Jamming*, abbreviated RoJ, is the main metric of interest in this work. It is defined as the ratio of number of jammed packets to the total number of transmitted packets. Given a and T, the jamming rate is $RoJ = a/T$. For each studied RAA, 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, whereas a high RoJ implies that the RAA is resilient. Note that a constraint on RoJ leads to the issue of choosing the optimal value of a (and corresponding value of T) that causes the maximum throughput degradation.

Utilization of the jamming rate metric can be justified by referring to the extensive literature on jamming attacks. According to [12], 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 [15].

The low volume of the RoQ attack makes it more difficult to effectively identify the attack. In addition, packet losses due to wireless channel conditions and interference could further decrease the possibility of detection. Thus, minimizing RoJ value ensures higher energy efficiency and lower probability of detection. We stress, nevertheless, that sophisticated detection schemes may still be capable of identifying such jammers [11, 37].

In this work, we discuss jamming strategies that work no matter what the channel characteristics are. According to our model, the jammer does not have any real-time knowledge of packet transmission results. The jammer does not need to detect these packet losses to apply the proposed strategies.

4. Analysis of RAAs under Jamming

In this section, we analyze the effects of jamming on the throughput of ARF and SampleRate. Note that several other rate adaptation algorithms, such as AARF and Onoe, are also vulnerable to periodic jamming. Their analysis can be found in our technical report [20]. We provide upper bounds on the jamming rates required to keep the throughput of each algorithm below the base rate. Our analysis applies to general parameter settings of the RAAs, under both perfect and lossy channels. In the following, RoJ_{RAA} denotes the jamming rate required to keep the throughput of RAA scheme below R_1, and Thr_{RAA} denotes the resulting throughput.

4.1. Automatic Rate Fallback (ARF)

ARF is the first documented rate adaptation algorithm [4]. It keeps track of the number of consecutive packet transmissions and failures at the current bit-rate. If s consecutive packet transmissions are correctly acknowledged, a probe packet is sent at the next higher rate (if available). If the probe packet succeeds, then the next higher bit-rate is used for subsequent frame transmissions. Otherwise, ARF returns back to the previous bit-rate. [4] refers to a probe packet failure as an *immediate fallback*. On the other hand, if f consecutive packet transmissions are not correctly acknowledged, the next lower bit-rate (if available) is used for subsequent frames. ARF is initiated from the lowest bit-rate possible R_1. The default values of the parameters of ARF are $s = 10$ and $f = 2$. In our analysis, we assume that both s and f are integers greater than 1. To keep the throughput lower than or equal to R_1, a simple strategy is to jam every probe packet (i.e., one out every $s + 1$ packets).

The jamming rate and the resulting throughput value of this strategy are provided by Proposition 1 that follows. The analysis of other (usually less effective) strategies can be found in [20].

Proposition 1. *The throughput of ARF can be kept below R_1 by using a bursty periodic jammer with jamming rate:*

$$RoJ_{ARF} = \frac{1}{s+1} .$$

PROOF. We begin our proof by assuming perfect channel conditions. The jamming strategy under consideration allows s consecutive successful transmissions at R_1, but jams each probe packet sent at R_2. For this purpose, a jammer can set a jamming period of $T = s + 1$ packets and burst size $a = 1$. Since each probe packet sent at R_2 is jammed, ARF is never able to switch to R_2 for further transmissions, resulting in:

- $\alpha_1 = \dfrac{s}{s+1}$, $\alpha_2 = RoJ_{\text{ARF}} = \dfrac{1}{s+1}$,
- $\phi_1 = 0$, $\phi_2 = 1$.

Using Eq. (1), we can calculate $Thr_{\text{ARF}} = s(s+1)^{-1}R_1$. This jamming strategy works also for *lossy channel* conditions. If any packet transmission at R_1 is lost within a jamming period, the system is not able to get s consecutive successful transmissions and does not even attempt to transmit at R_2. □

For default parameter values (i.e., $s = 10$ and $f = 2$), $RoJ_{\text{ARF}} \approx 9.1\%$.

Next, we show that the bound of Proposition 1 is near optimal if $R_2 \geq 2R_1$. This assumption holds for most IEEE 802.11 standards, including IEEE 802.11g, IEEE 802.11n, and IEEE 802.11ac.

Proposition 2. *Suppose $R_2 \geq 2R_1$. Then the rate of jamming of the optimal jamming strategy against ARF is at least $1/(s+2)$ for any $s \geq 1$ and $f \geq 1$.*

PROOF. Consider the bursty periodic jamming strategy against ARF described in the proof of Proposition 1, which is denoted as strategy J. Strategy J guarantees that (i) all successful transmissions occur only at the lowest possible rate R_1; (ii) The number of consecutive successful transmissions at

rate R_1 is maximized (i.e., no other strategy leads to more consecutive successful transmissions at rate R_1).

Now suppose there exists another jamming strategy, call it O, with lower rate of jamming than J. Strategy O would therefore necessarily allow transmissions at higher bit rates. Since $R_2 \geq 2R_1$, each successful packet transmission at rate higher than R_1 must be compensated by the jamming of at least one packet. Therefore the jamming rate of strategy O must be at least $1/(s+2)$ (i.e, s packets transmitted at rate R_1, one packet transmitted at rate R_2, and one packet jammed). Note that a strategy achieving this lower bound is feasible if $f = 1$. □

From Proposition 2, we deduce that, for default parameters, the optimal jamming rate against ARF must be at least 8.3%.

4.2. SampleRate

SampleRate [3], an algorithm implemented on MadWifi card adapters [38], estimates the expected per-packet transmission time at each bit-rate, and selects the bit-rate that is predicted to achieve the highest throughput. To get the estimates, it periodically sends packets at transmission rates other than the current one and records the transmission times. SampleRate switches to another bit-rate if the estimated average per-packet transmission time at that rate is smaller than that at the current bit-rate. Furthermore, bit-rates expected to perform worse, i.e. with minimum transmission times higher than the average transmission time of the current bit-rate, are not sampled. Results of transmissions that occurred over $updWin$ (default 10) seconds ago are discarded.

If no packets have been acknowledged at the current bit-rate, SampleRate picks the highest bit-rate that has not had four consecutive failures. Furthermore, a rate that had four consecutive failures is blacklisted, i.e. SampleRate does not pick it for $updWin$ seconds. Thus, preventing any transmission at rates higher than R_1 will cause all rates but R_1 to be blacklisted, keeping the system at R_1 for $updWin$ seconds.

A possible jamming strategy to keep the throughput of SampleRate below R_1 is to jam every packet transmitted at a bit-rate higher than R_1. The jamming rate and the resulting throughput value of this strategy are calculated in the proof of Proposition 3. We assume the packet length is set to $pktL$.

Proposition 3. *The throughput of SampleRate can be kept below R_1 by a bursty periodic jammer with jamming rate:*

$$RoJ_{SampleRate} = \frac{4(n-1)pktL}{4(n-1)pktL + updWin \times R_1} \,. \tag{2}$$

PROOF. We begin our proof by assuming perfect channel conditions. Since four packet failures are necessary to blacklist any rate, one needs to jam $a = 4(n-1)$ packets consecutively to blacklist all bit-rates higher than R_1. This causes the system to get stuck at R_1 for $updWin$ seconds. Since the jamming period consists of transmissions performed at rate R_1 for $updWin$ seconds and $4(n-1)$ packet transmissions at higher rates, $T = R_1\ updWin(pktL)^{-1} + 4(n-1)$, leading to the RoJ expression given by Eq. (2). The resulting values are:

- $\alpha_1 = 1 - RoJ_{\text{SampleRate}}$, $\sum_{i=2}^{n} \alpha_i = RoJ_{\text{SampleRate}}$,
- $\phi_1 = 0$, $\phi_2 = \phi_3 = \ldots = \phi_n = 1$.

Using Eq. (1), we can calculate the throughput:

$$Thr_{\text{SampleRate}} = \left[\frac{R_1 \times updWin}{4(n-1)pktL + R_1 \times updWin} \right] R_1 \,.$$

This jamming strategy works also for *lossy channel* conditions. Once SampleRate is forced down to R_1, all bit-rates higher than R_1 are blacklisted. Packet losses at R_1 within $updWin$ seconds do not affect the behavior of SampleRate, since only R_1 is available. As soon as higher bit-rates are available, SampleRate switches to those rates regardless of any packet loss that might have occurred in the last update window. Jamming the transmissions at higher bit-rates forces SampleRate to go down to R_1 again. □

For default parameter values (i.e., $n = 12$, $pktL = 10000$ bits, $updWin = 10$ sec and $R_1 = 1$ Mb/s), $RoJ_{\text{SampleRate}} \approx 4.2\%$.

5. Jamming-Resistant Rate Adaptation

In the previous section, we analyzed the vulnerability of existing RAAs to periodic jamming attacks. Our next objective is to develop a robust RAA that offers stronger protection against jammers, that is, the RoJ against such RAAs is guaranteed to exceed a minimum threshold (which, by design, should be as high as possible). Offering such a guarantee is non-trivial, since it must hold for all possible settings of the jamming parameters that satisfy the RoJ constraint. Moreover, the robust RAA should perform similarly to non-robust RAAs in the absence of jammers.

In this section, we propose a plausible approach for a robust RAA, called Randomized ARF (RARF), and analyze its performance under the bursty periodic model. Although we assume perfect channel conditions at first, we generalize our analysis to lossy channel conditions later. We derive a closed-form lower bound on the minimum jamming rate required to keep RARF throughput below R_1 (i.e., no matter how the adversary selects the values of T and a, the jamming rate must be at least as high as this bound). This bound is much higher than the jamming rate sufficient to keep the throughput of ARF and SampleRate below R_1.

5.1. Randomized ARF (RARF)

In Section 4.1, we have shown that the throughput of ARF can be kept below R_1 if $RoJ = (s+1)^{-1}$. The main reason for this vulnerability is the deterministic nature of ARF. Since the adversary knows exactly when ARF jumps to R_2, and when it comes down to R_1 after jamming, it is easy to employ a jamming strategy that keeps the throughput of ARF below R_1. However, randomizing the location of these jumps prevents the adversary to decide which packets to jam. Thus, instead of switching to the next higher rate after s successful transmissions, RARF switches with probability $\Pr(switch) = s^{-1}$ after each successful transmission. In our subsequent analysis, we refer to these probability trials as *coin flips*. The failure mechanism of RARF is the same as ARF, i.e. RARF switches to the next lower rate after f consecutive failures at the current bit-rate. RARF does not make use of probe packets, however.

Note that randomized protocols may be harder to troubleshoot or police than deterministic protocols. Yet, they are already commonplace in wireless networks. For instance, IEEE 802.11 use random back-offs to arbitrate channel contention. Even in the context of RAAs, randomized algorithms have

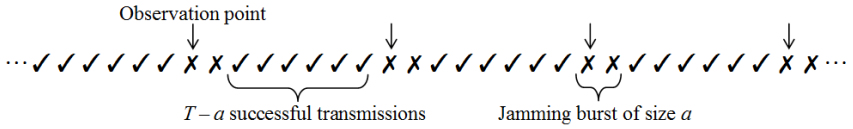


Figure 1: Diagram of the observation process

already been proposed and implemented in drivers [6]. Our main contributions lie in judiciously applying randomization into an existing RAA and in theoretically analyzing the robustness properties of its randomized version.

5.2. Throughput of RARF

In this section we derive an expression for the expected throughput of RARF. In Section 5.3, we use this expression to derive a lower bound on the minimum rate of jamming needed to keep the throughput of RARF below R_1. We initially assume that RARF operates only over two bit-rates (R_1 and R_2). The lower bound on RoJ can easily be shown to apply to multiple bit-rates, as explained in Section 5.4.

We observe the system just before the jamming burst in every jamming period. The state of the system is the transmission rate used at the time of observation, thus the state space is $S = \{R_1, R_2\}$. A diagram for the observation process is given in Fig. 1. Check marks indicate successful transmissions while cross marks stand for failed transmissions due to jamming. The steady state probability of finding the system at rate R_i is denoted as π_i.

The behavior of the system depends on the burst size a. Thus, we consider two different cases for the adversary: $a < f$ and $a \geq f$. We start with the simpler case, when $a < f$.

Proposition 4. *Under a bursty periodic jammer with parameters (a, T) and $a < f$, the throughput of two-rate RARF is:*

$$\mathbb{E}[Thr_{RARF}] = \left(\frac{T-a}{T}\right) R_2 \ .$$

Proof. RARF switches to the next lower rate only when f consecutive failures occur. Thus, if the system switches to R_2 at some point, it stays at R_2 until the end of transmission, since the jammer cannot force the system down to the next lower rate with a jamming burst size of $a < f$. In addition, a bursty periodic jammer allows at least one successful transmission

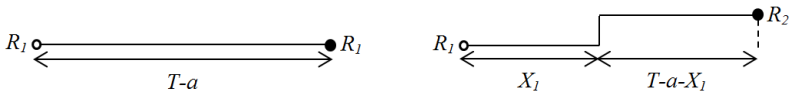


Figure 2: Possible scenarios in a jamming period when $a \geq f$.

in each jamming period ($T > a$). Since RARF switches to R_2 with a non-zero probability after each successful transmission at R_1, it is impossible to keep RARF at R_1 forever using a bursty periodic jammer. Therefore, RARF switches to R_2 no matter what the jammer parameters are, and stays at R_2 if $a < f$. Since we consider the steady state throughput, we ignore the temporary phase until RARF switches to R_2, resulting in the following values:

- $\alpha_1 = 0$, $\alpha_2 = 1$,
- $\phi_2 = \dfrac{a}{T}$.

Using Eq. (1), we can calculate the throughput:

$$\mathbb{E}[Thr_{\text{RARF}}] = \left(\frac{T-a}{T}\right) R_2 \ .$$

□

Next, we analyze the case $a \geq f$. This time, RARF is guaranteed to be at R_1 after each jamming burst. If the bit-rate at the observation point is R_1, all $T - a$ packets before that point must have been transmitted at R_1 as in Fig. 2(a), since the jammer was idle during those transmissions. On the other hand, if the current bit-rate is R_2, some of the last $T - a$ packets were transmitted at R_1 and the rest were transmitted at R_2 as in Fig. 2(b). X_1 denotes the number of packets transmitted at rate R_1 in a jamming period, given that the bit-rate right before the jamming burst is R_2. Next, we provide an expression for the expectation of X_1.

Lemma 1.

$$\mathbb{E}[X_1] = s - \frac{(T-a)\left(1-\frac{1}{s}\right)^{T-a}}{1-\left(1-\frac{1}{s}\right)^{T-a}} \ .$$

PROOF. By definition of X_1, it is given that the bit-rate right before the jamming burst is R_2. If it was not given, the number of packets transmitted at R_1 would have a geometric distribution, since each coin flip after a successful transmission is independent of the others. Let Y_1 denote this geometric random variable with the following distribution:

$$\begin{aligned}\Pr(Y_1 = y) &= \Pr(switch)[1 - \Pr(switch)]^{y-1} \\ &= \frac{1}{s}\left(1 - \frac{1}{s}\right)^{y-1}, \quad \text{for } y = 1, 2, \ldots \end{aligned} \tag{3}$$

However, we know that the system uses a higher bit-rate after $T-a$ packet transmissions, thus a transition must have occurred before that. This limits the set of possible values for X_1 to the set $\{1, 2, \ldots, T-a\}$. Therefore, we can denote X_1 as a truncated geometric random variable with the following distribution:

$$p_{X_1}(x) = \frac{\Pr(Y_1 = x)}{\Pr(Y_1 \leq T-a)} = \frac{\frac{1}{s}\left(1 - \frac{1}{s}\right)^{x-1}}{1 - \left(1 - \frac{1}{s}\right)^{T-a}}, \tag{4}$$

for $x = 1, 2, \ldots, T-a$. Using Eq. (4), we can calculate the expected value of X_1 as follows:

$$\mathbb{E}[X_1] = \frac{\sum_{x=1}^{T-a} \frac{x}{s}\left(1 - \frac{1}{s}\right)^{x-1}}{1 - \left(1 - \frac{1}{s}\right)^{T-a}} = s - \frac{(T-a)\left(1 - \frac{1}{s}\right)^{T-a}}{1 - \left(1 - \frac{1}{s}\right)^{T-a}}.$$

□

Next, we provide expressions for the probability of finding the system at rate R_1 or rate R_2, at the time of an observation.

Lemma 2. *Under a bursty periodic jammer with parameters (a, T) and $a \geq f$, the steady state probabilities for a two-rate RARF system are:*

$$\pi_1 = \left(1 - \frac{1}{s}\right)^{T-a}, \qquad \pi_2 = 1 - \left(1 - \frac{1}{s}\right)^{T-a}.$$

PROOF. For $a \geq f$, we know that the system starts transmission from R_1 after every jamming burst. Thus, the probability that we observe the system at R_1 is equal to the probability that all coin flips between two observation points fail. We know that there are T packet transmissions between two observation points but a of them are jammed. Thus, we have $T-a$ coin flips between two observations, leading to:

$$\pi_1 = [1 - \Pr(switch)]^{T-a} = \left(1 - \frac{1}{s}\right)^{T-a},$$
$$\pi_2 = 1 - \pi_1 = 1 - \left(1 - \frac{1}{s}\right)^{T-a}.$$

□

Applying the previous two lemmas, the following theorem provides an expression for the throughput of RARF.

Theorem 1. *Under a bursty periodic jammer with parameters (a, T) and $a \geq f$, the throughput of two-rate RARF is:*

$$\mathbb{E}[Thr_{RARF}] = \left(\frac{T-a}{T}\right) R_2 - \left[1 - \left(1 - \frac{1}{s}\right)^{T-a}\right] \frac{s\,(R_2 - R_1)}{T}.$$

PROOF. We consider the successful transmissions during the last jamming period given the bit-rate at the current observation point. The current state can either be R_1 or R_2 with probabilities π_1 and π_2 given by Lemma 2. If the current state is given as R_1, then all successful transmissions in the previous jamming period are guaranteed to be transmitted R_1 as in Fig. 2(a).

On the other hand, if the current state is given as R_2, then we know that a transition has definitely occurred in the last jamming period as in Fig. 2(b). The transition happens after X_1 packets are transmitted at R_1, and the remaining $T - a - X_1$ successful packet transmissions use R_2. Lastly, Lemma 1 gives the expected value of the location of this transition, leading to the following expected throughput value:

$$\begin{aligned}
\mathbb{E}[Thr_{\mathrm{RARF}}] &= \pi_1 \left(\frac{T-a}{T}\right) R_1 + \pi_2 \left(\frac{\mathbb{E}[X_1]}{T} R_1 + \frac{T-a-\mathbb{E}[X_1]}{T} R_2\right) \\
&= \left(1-\frac{1}{s}\right)^{T-a} \left(\frac{T-a}{T}\right) R_1 \\
&+ \left[1-\left(1-\frac{1}{s}\right)^{T-a}\right] \left(\frac{\mathbb{E}[X_1]}{T} R_1 + \frac{T-a-\mathbb{E}[X_1]}{T} R_2\right) \qquad (5) \\
&= \left(\frac{T-a}{T}\right) R_2 - \left[1-\left(1-\frac{1}{s}\right)^{T-a}\right] \frac{s\,(R_2-R_1)}{T} \,.
\end{aligned}$$

□

5.3. Jamming Strategies Against RARF

In this section, we derive a lower bound on the minimum rate of jamming needed for a bursty periodic jammer to cause the throughput of RARF to fall below R_1. First, we analyze the simple case $a < f$.

Proposition 5. *For $a < f$, the throughput of RARF can be kept below R_1 by using a bursty periodic jammer with jamming rate:*

$$RoJ_{RARF} = 1 - \frac{R_1}{R_2} \,.$$

For default parameter values (i.e., $R_1 = 1$ Mb/s and $R_2 = 2$ Mb/s), $RoJ_{RARF} = 50\%$.

Proof. Using the expected throughput expression given by Proposition 4, we can calculate the lowest RoJ to keep that expression less than or equal to R_1 as follows:

$$\mathbb{E}[Thr_{\mathrm{RARF}}] = \left(\frac{T-a}{T}\right) R_2 = (1 - RoJ_{\mathrm{RARF}})\, R_2 \leq R_1 \,,$$

$$RoJ_{\mathrm{RARF}} \geq 1 - \frac{R_1}{R_2} \,.$$

□

Unless R_2 is close to R_1, choosing $a < f$ requires a high jamming rate to keep the throughput below R_1. Thus, the case $a \geq f$ usually results in a more efficient jamming strategy.

The throughput expression given by Theorem 1 for $a \geq f$ appears complicated for deriving an expression for RoJ. Thus, we use a lower bound on the throughput of RARF that in turn will be used to derive a lower bound on the minimum jamming rate. This bound is based on the following lemma:

Lemma 3.

$$\mathbb{E}[X_1] \leq \frac{T-a+1}{2} \ .$$

PROOF. Using Eq. (4), we can write the cumulative distribution function (CDF) of X_1 as follows:

$$F_{X_1}(x) = \frac{1-\left(1-\frac{1}{s}\right)^x}{1-\left(1-\frac{1}{s}\right)^{(T-a)}} \ , \quad \text{for } x = 1, 2, \ldots, T-a.$$

The expected value of X_1 can be calculated as:

$$\mathbb{E}[X_1] = \sum_{x=1}^{T-a} \mathbb{P}(X_1 \geq x) = \sum_{x=0}^{T-a} 1 - F_{X_1}(x) \ .$$

Let's consider another discrete random variable Z_1 that is distributed uniformly over the same region. The CDF of Z_1 is given as follows:

$$F_{Z_1}(z) = \frac{z}{T-a} \ , \quad \text{for } z = 1, 2, \ldots, T-a.$$

The expected value of Z_1 can be calculated as:

$$\mathbb{E}[Z_1] = \sum_{z=1}^{T-a} \mathbb{P}(Z_1 \geq z) = \sum_{z=0}^{T-a} 1 - F_{Z_1}(z) = \frac{T-a+1}{2} \ .$$

We know the following about X_1 and Z_1:

- Both X_1 and Z_1 are defined over the same region.
- Since X_1 is a truncated geometric random variable, $F_{X_1}(y)$ is concave over $y \in [0, T-a]$.
- Since Z_1 is a uniform random variable, $F_{Z_1}(y)$ is linear over $y \in [0, T-a]$.

- $F_{X_1}(0) = F_{Z_1}(0) = 0$.
- $F_{X_1}(T-a) = F_{Z_1}(T-a) = 1$.

Thus, one can deduce that:

$$F_{X_1}(y) \geq F_{Z_1}(y)\ , \quad \text{for } y = 1, 2, \ldots, T-a\ ,$$
$$\mathbb{E}[X_1] \leq \mathbb{E}[Z_1] = \frac{T-a+1}{2}\ .$$

□

In order to find the optimum rate of jamming, we need to find optimum values for a and T separately. Instead, we first keep the jamming rate fixed at a'/T'. Later, we evaluate the expected throughput value of RARF under a bursty periodic jammer with parameters (ka', kT'), where k is a real number greater than or equal to 1. Finally, we show that the expected throughput increases with k, urging the jammer to pick the lowest possible value of a if RoJ is fixed.

Lemma 4. *For a bursty periodic jammer (a, T) with a fixed jamming rate and for $a \geq f$, a lower bound on the throughput of two-rate RARF is minimized when $a = f$.*

Proof. As we have mentioned before, we consider a bursty periodic jammer with parameters (ka', kT'), where $k \geq 1$. Using Eq. (5), we can express the expected throughput of two-rate RARF scheme under this jammer as follows:

$$\mathbb{E}[Thr_{\text{RARF}}] = \left(1 - \frac{1}{s}\right)^{k(T'-a')} \left(1 - \frac{a'}{T'}\right) R_1 + \left[1 - \left(1 - \frac{1}{s}\right)^{k(T'-a')}\right] \left[\frac{\mathbb{E}[X_1]}{kT'} R_1 + \left(1 - \frac{a'}{T'} - \frac{\mathbb{E}[X_1]}{kT'}\right) R_2\right].$$

Applying Lemma 3 to Eq. (5) yields a lower bound on the throughput of RARF. Note that an upper bound on $\mathbb{E}[X_1]$ implies a lower bound on the expected throughput, since the system throughput drops if more time is spent at R_1.

$$\begin{aligned}\mathbb{E}[Thr_{\text{RARF}}] \geq & \left[1+\left(1-\frac{1}{s}\right)^{k(T'-a')}\right]\left(1-\frac{a'}{T'}\right)\frac{R_1}{2} \\ & + \left[1-\left(1-\frac{1}{s}\right)^{k(T'-a')}\right]\left[\left(1-\frac{a'}{T'}\right)\frac{R_2}{2}-\frac{R_2-R_1}{2kT'}\right] \\ & = \beta_1(k)\left(1-\frac{a'}{T'}\right)\frac{R_1}{2}+\beta_2(k)\left(1-\frac{a'}{T'}\right)\frac{R_2}{2}\,,\end{aligned}$$

where

$$\beta_1(k) = 1+\frac{1}{k(T'-a')}+\left[1-\frac{1}{k(T'-a')}\right]\left(1-\frac{1}{s}\right)^{k(T'-a')},$$

$$\beta_2(k) = \left[1-\frac{1}{k(T'-a')}\right]\left[1-\left(1-\frac{1}{s}\right)^{k(T'-a')}\right].$$

Note that increasing the value of k causes β_1 to decrease, and β_2 to increase, leading to an increase in the expected throughput. Therefore, for a fixed jamming period, a bursty periodic jammer with parameters (a, T) should choose the value of a as low as possible within the acceptable region, in order to obtain the lowest throughput of the two-rate RARF system. In our case, the lowest possible value of a is f, since the operating region is $a \geq f$.□

Lemma 4 reduces the two dimensional optimization problem to a one dimensional integer programming problem [39]. However, keeping $a = f$ and solving for T might not result in an integer value. Since our purpose is to derive a lower bound on *RoJ* rather than choosing jammer parameters, we relax the problem by considering non-integer values for T, keep $a = f$, and calculate the bound on *RoJ* accordingly.

At this point, we know that the optimal value of a in the region $a \geq f$ is equal to f. Thus, we have to find the corresponding optimal value of T. Lemma 5 helps in further simplifying the expression of $\mathbb{E}[Thr_{\text{RARF}}]$.

Lemma 5.

$$\left(1-\frac{1}{s}\right)^{x} \leq \frac{s}{e\,x}\,, \qquad \textit{for } s \geq 2 \textit{ and } x \geq 1,$$

where e is Euler's number.

The proof of Lemma 5 can be found in the Appendix. Using the result of Lemma 5, Theorem 2 provides a closed-form expression for a lower bound on RoJ_{RARF}.

Theorem 2. *To keep the throughput of RARF below R_1, a bursty periodic jammer with $a \geq f$ must satisfy the following:*

$$RoJ_{RARF} \geq \frac{f}{\frac{b+\sqrt{b^2-4es}}{2e} + f},$$

where $b = e + s + \dfrac{2ef}{\frac{R_2}{R_1} - 1}$.

Proof. Applying Lemmas 3, 4 and 5 on Eq. (5) results in the following bound on the throughput:

$$\mathbb{E}[Thr_{\text{RARF}}] \geq \frac{T-f}{2T}\left\{R_2 + R_1 - \left(\frac{R_2 - R_1}{T-f}\right)\left[1 + \frac{s}{e} - \frac{s}{e(T-f)}\right]\right\}.$$

Setting this bound below R_1 yields an upper bound on T. Let $x = T - f$.

$$\frac{x}{2(x+f)}\left[R_2 + R_1 - (R_2 - R_1)\left(\frac{1}{x} + \frac{s}{e\,x} - \frac{s}{e\,x^2}\right)\right] \leq R_1,$$

leading to the following quadratic expression:

$$ex^2 - \left(e + s + \frac{2ef}{\frac{R_2}{R_1} - 1}\right)x + s \leq 0. \tag{6}$$

Let $b = e + s + \dfrac{2ef}{\frac{R_2}{R_1} - 1}$.

The two roots of Eq. (6) are denoted by x_1 and x_2. Since x_1 is always smaller than 1, the only feasible root is:

$$x_2 = \frac{b + \sqrt{b^2 - 4es}}{2e},$$

resulting in the following bound on the jamming rate:

$$RoJ_{\text{RARF}} = \frac{f}{T} \geq \frac{f}{x_2 + f} = \frac{f}{\frac{b+\sqrt{b^2-4es}}{2e} + f}.$$

□

For default parameter values (i.e. $s = 10$, $f = 2$, $R_1 = 1$ Mb/s and $R_2 = 2$ Mb/s), we get $b \approx 23.59$ and $RoJ_{\text{RARF}} \geq 19.5\%$. Apart from an analytical bound, a slightly tighter numerical bound on RoJ_{RARF} can be derived as in Theorem 3.

Theorem 3. *A lower bound on RoJ_{RARF} can be found by keeping $a = f$ and solving for the largest T value that satisfies the following inequality:*

$$T - f + se^{-\frac{s+1}{s^2}(T-f)} \leq \frac{f}{\frac{R_2}{R_1} - 1} + s \ .$$

given that $R_2 \leq (f+1)R_1$.

The proof of Theorem 3 can be found in the Appendix. For default parameter values (i.e., $s = 10$, $f = 2$, $R_1 = 1$ Mb/s and $R_2 = 2$ Mb/s), $T \leq 9.714$ and $RoJ_{\text{RARF}} \geq 20.6\%$.

Combining Theorem 2 and Proposition 5, we can pick the smaller of the two expressions as a lower bound on the optimal jamming rate. For default parameter values, our analysis formally proves that a bursty periodic jammer attacking RARF must at least double the jamming rate compared to ARF. For IEEE 802.11g networks, our ns-3 simulations in Section 6 show that the difference between the minimum jamming rates of RARF and ARF is even higher, i.e. about 33% for RARF versus 9% for ARF.

Note that any jamming strategy that is able to keep RARF throughput below R_1 under perfect channel conditions works under any channel model too. This is because any packet loss at R_1 within a jamming period might delay the switch to R_2, resulting in a lower throughput. Although, a lower RoJ value might be enough, the jammer should always utilize the strategy employed for the perfect channel to make sure that the throughput is lower than R_1.

5.4. Generalization of Results to Multiple Rates

Until this point, we have only considered a two-rate RARF scheme. In this section, we generalize our results to an n-rate system, where $n \geq 2$. We use a coupling method to compare the two-rate system and the n-rate system, i.e. each coin flip has the same result at both systems. We assume that both systems start from R_1.

We again consider different cases for the burst size of the jammer. The first case is when $a \geq (n-1)f$. In this case, both systems are guaranteed

to be at R_1 right after a jamming burst, and since we are using the coupling method, both systems switch to R_2 at the same instant. However, the n-rate system can switch to higher bit-rates after this point, whereas the two-rate system gets stuck at R_2 until the next jamming burst.

$(\alpha_i)_{n-rate}$ denotes the long run proportion of packets transmitted at R_i where n bit-rates are available. Since the jamming pattern, results of the coin flips, and the number of packets sent at R_1 are the same for both systems, we can derive the following:

For $a \geq (n-1)f$

- $(\alpha_1)_{2-rate} = (\alpha_1)_{n-rate}$,
- $(\alpha_2)_{2-rate} = \sum_{i=2}^{n} (\alpha_i)_{n-rate}$.

When $f \leq a < (n-1)f$, the two-rate system is guaranteed to be at R_1 right after a jamming burst. On the other hand, the n-rate system may or may not drop down to R_1 after jamming, leading to:

For $f \leq a < (n-1)f$

- $(\alpha_1)_{2-rate} \geq (\alpha_1)_{n-rate}$,
- $(\alpha_2)_{2-rate} \leq \sum_{i=2}^{n} (\alpha_i)_{n-rate}$.

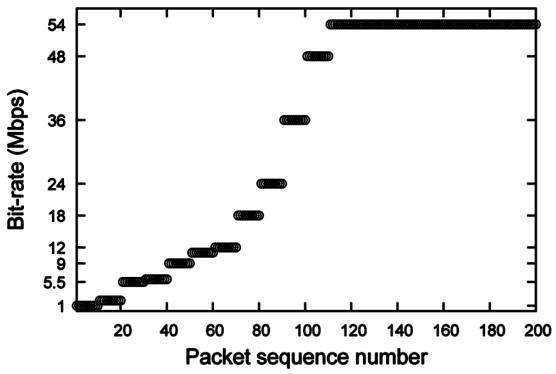
Lastly, when $a < f$, both systems get stuck at the highest bit-rate possible throughout the transmission, resulting in the following values:

For $a < f$

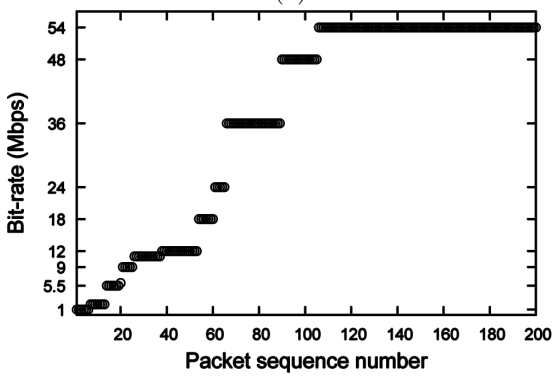
- $(\alpha_2)_{2-rate} = (\alpha_n)_{n-rate} = 1$,
- $(\alpha_1)_{2-rate} = (\alpha_1)_{n-rate} = \ldots = (\alpha_{n-1})_{n-rate} = 0$.

Based on Eq. (1) and the resulting α_i values, the following expression holds for all values of a:

$$\mathbb{E}[Thr_{\text{RARF}}]_{n-rate} \geq \mathbb{E}[Thr_{\text{RARF}}]_{2-rate} \tag{7}$$



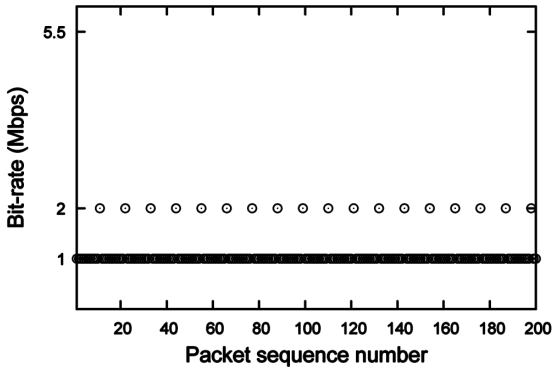
(a)



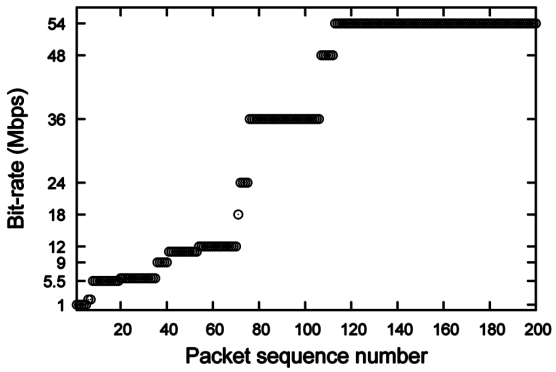
(b)

Figure 3: Performance under perfect channel with no jamming: (a) ARF, $Thr = 53.980$ Mb/s, (b) RARF, $Thr = 53.984$ Mb/s. ARF and RARF perform similarly in the absence of a jammer.

Eq. (7) shows that for any given bursty periodic jamming strategy, the throughput of n-rate RARF is higher than that the throughput of two-rate RARF. Therefore, the lower bounds on the rate of jamming derived in Section 5.3 for two-rate RARF apply also to n-rate RARF. Note that RoJ of n-rate RARF cannot be lower than RoJ of two-rate RARF since otherwise Eq. (7) would not hold for the optimal bursty periodic jamming strategy against n-rate RARF.



(a)



(b)

Figure 4: Performance under perfect channel with bursty periodic jamming: (a) ARF under jamming with $a = 1$ and $T = 11$, $Thr = 0.909$ Mb/s ; and (b) RARF under jamming with $a = 1$ and $T = 11$, $Thr = 49.072$ Mb/s. RARF performs markedly better than ARF in the presence of a jammer.

6. NS-3 Simulations

6.1. Set-up

In this section, we present the results of ns-3 simulations [40] 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 bursty periodic jamming strategy. We present first present results for lossless channels and then for lossy channels, both without and with jammers.

We use standard ns-3 libraries whenever possible. We build new ns-3

modules for SampleRate and RARF algorithms, since they are not available. In all our simulations, we set the length of each DATA packet to 1250 bytes. We use IEEE 802.11g in ad-hoc mode since we consider two stations and wish to avoid beacons.

The network topology that we consider is as follows. We consider two legitimate nodes A and B, where A aims to send packets to B continuously. The jammer node is located between A and B, and has the same transmission power as them. Whenever A tries to send a packet to B, the jammer detects it and decides whether to corrupt the packet or not, based on the parameter values a and T.

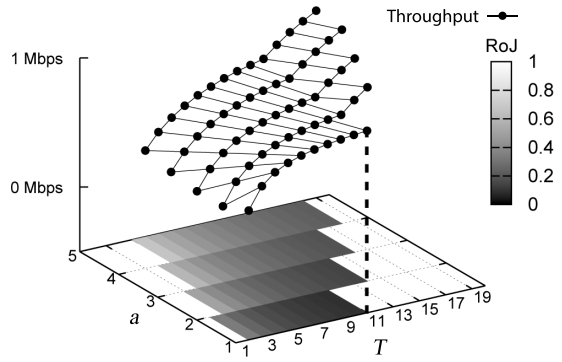
Although our ns-3 simulations take into consideration control packets, back-off retransmissions, and inter-frame spacings, the resulting throughput values are based on our definition in Section 3.1.

6.2. ARF and RARF

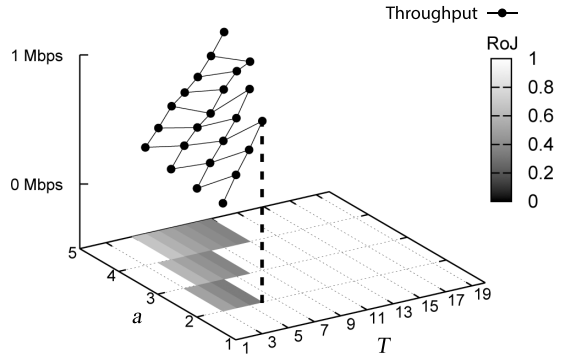
In this section, we compare the performances of ARF and RARF. Simulations are run for 100 seconds under a perfect channel, and the first 200 DATA packet transmissions are plotted in Figures 3 and 4. In Fig. 3(a) and Fig. 3(b), respective performances of ARF and RARF are shown in the absence of a jammer. One can observe that the algorithms take similar time to converge to the highest bit-rate and continue transmitting at that rate henceforth.

In Fig. 4(a) the performance of ARF is tested under the jamming strategy given by Theorem 1. The resulting throughput is 0.909 Mb/s. One can see that each probe packet sent at 2 Mb/s is jammed. Fig. 4(b) illustrates the performance of RARF under the same jamming strategy. In that case, the jammer fails to keep the system at low rates and the resulting throughput value is 49.072 Mb/s. This result shows that an effective jamming strategy against ARF does not have much effect on RARF.

In Fig. 5, throughput values of ARF and RARF under a bursty periodic jammer are plotted with a and T taken as parameters. This figure intends to indicate jamming strategies that keep ARF and RARF throughput below the base-rate, rather than comparing the performance of these two RAAs under general jamming parameters. The jamming period $T \in \{1, 2, \ldots, 20\}$, and the jamming burst size $a \in \{1, 2, \ldots, 5\}$. The resulting throughput values that are lower than or equal to 1 Mb/s are plotted. The jamming rate RoJ is illustrated as a contour plot for valid jamming strategies at the bottom of each figure. Note that each data point indicates a jamming strategy that



(a)



(b)

Figure 5: Throughput of (a) ARF and (b) RARF under periodic jamming with parameters a and T. RoJ is depicted as a contour plot at the bottom of each graph. Low RoJ values are plotted in dark colors to indicate the severity of the vulnerability. Among the strategies to keep the throughput below 1 Mb/s, the one with the lowest RoJ is indicated.

manages to keep the throughput below R_1. The optimal strategy should have the lowest RoJ among those.

In Fig. 5(a) for ARF, RoJ is minimized when $a = 1$ and $T = 11$, as given by Proposition 1. On the other hand, Fig. 5(b) reveals that the optimal jamming strategy against RARF has the parameters $a = 2$ and $T = 6$, resulting in a rate of jamming of 33.3%. Thus, any jamming strategy with RoJ below 33.3% fails to keep the throughput of RARF below 1 Mb/s.

Table 1 shows that RoJ_{RARF} is sizably higher than the lower bound de-

RAA	Analytical Results	Simulation Results
ARF	$RoJ = 9.1\%$	$RoJ = 9.1\%$
SampleRate	$RoJ = 4.2\%$	$RoJ = 4.7\%$
RARF	$RoJ \geq 19.5\%$	$RoJ = 33.3\%$

Table 1: Analytical and simulation results for minimum jamming rate to keep the throughput of each RAA below 1 Mb/s.

rived in Theorem 2, since twelve rates are available in IEEE 802.11g. On the other hand, ns-3 simulations of RARF with two bit-rates yield $a = 2$ and $T = 9$ as the optimal values. This leads to an RoJ of 22.2%, which is close to the analytical bound of 19.5% derived in Theorem 2 and the numerical bound of 20.6% derived in Theorem 3.

6.3. SampleRate

We consider the jamming strategy given by Theorem 3 for SampleRate. Simulation is run for 100 seconds under a perfect channel, and the first 50 seconds are plotted in Fig. 6. Each data point indicates the rate used for a DATA packet transmission. We use an initial jamming phase forcing the rate down to 1 Mb/s. Note that the only information needed in this initial phase is the time when the transmissions start, which can be obtained by carrier sensing.

The bursty periodic jammer corrupts 44 consecutive packets after every 10 seconds spent at 1 Mb/s. Since the transmission of acknowledgments take a non-negligible amount of time, the system transmits 890 packets in 10 seconds at 1 Mb/s rather than 1000 packets. The jammer parameters to keep SampleRate throughput below 1Mb/s are $a = 44$ and $T = 934$, leading to an RoJ value of 4.7%, close to the value of 4.2% predicted by Theorem 3.

We have also observed that such a jamming pattern cannot keep RARF throughput below 1Mb/s, since during 10 seconds of idle period of the jammer, RARF performs many jumps to rates higher than 1Mb/s.

6.4. Lossy Channel

In this section, we perform simulations for lossy channels utilizing the `ns3::LogDistancePropagation LossModel` of ns-3, which has the following parameters:

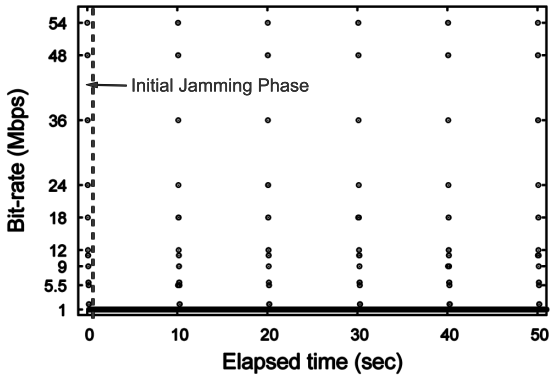


Figure 6: Performance of SampleRate under bursty periodic jamming with $a = 44$ and $T = 934$. $Thr = 0.955$ Mb/s.

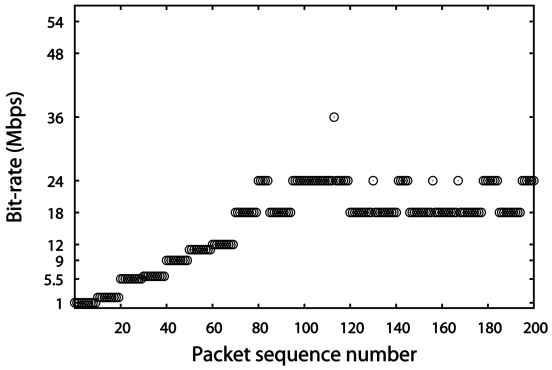
- k : path loss distance exponent,
- d_0 : reference distance (m),
- L_0 : path loss at reference distance (dB),
- d : distance (m),
- L : path loss (dB).

The reception power is calculated using the log-distance propagation loss model by the following equation:

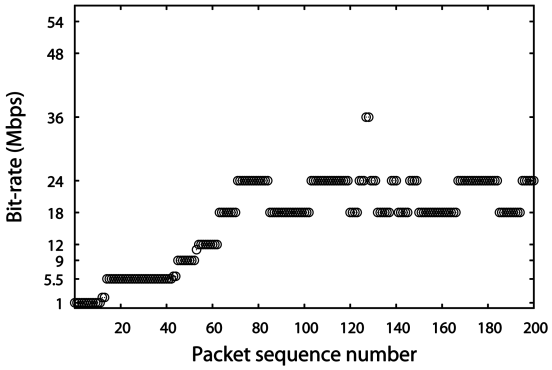
$$L = L_0 + 10\,k\,\log_{10}\left(\frac{d}{d_0}\right). \tag{8}$$

The default parameter values for this channel model are $k = 3$, $d_0 = 1\,m$, and $L_0 = 46.677$ dB. Under this channel model, we first compare the performances of ARF and RARF without jammers. The simulations are run for 100 seconds in the absence of a jammer with $d = 70\,m$ and default channel parameter values. Fig. 7 plots the rates used for the first 200 DATA packet transmissions for each RAA. One can observe that ARF and RARF perform similarly, leading to similar throughput values.

Next, we implement the jamming strategies devised in Sections IV and V for ARF, RARF, SampleRate with $d \in \{10, 20, \ldots, 200\}$, $k \in \{1, 2, \ldots, 5\}$, and default values for d_0 and L_0. We find that the jamming strategies manage to keep the throughput below 1 Mb/s for each RAA. As an example, throughput values for $d = 100\,m$ and $k = 3$ are given in Table 2.



(a)



(b)

Figure 7: Performance under lossy channel with no jamming: (a) ARF, $Thr = 21.77\,\text{Mb/s}$, (b) RARF, $Thr = 23.22\,\text{Mb/s}$. ARF and RARF perform similarly under lossy channel conditions in the absence of a jammer.

6.5. Alternative Throughput Definition

In Section 3.1, we have defined throughput as the average rate used per packet. This definition of throughput enabled us to perform exact analysis of the behavior of rate control mechanisms under various jamming patterns.

An alternative and widely used definition of throughput is the number of bits transmitted successfully per unit time. Assume that the packet length is fixed to $pktL$ and N packets are transmitted in total. Let N_i denote the number of packets transmitted at R_i, so that $\alpha_i = N_i/N$. In this case, the alternative throughput metric can be defined as:

RAA	Jammer Parameters	Thr
ARF	$a = 1$, $T = 11$	0.909 Mb/s
SampleRate	$a = 44$, $T = 934$	0.951 Mb/s
RARF	$a = 2$, $T = 6$	0.895 Mb/s

Table 2: Throughput values of various RAAs with corresponding effective jamming strategies under a lossy channel. The strategies considered for perfect channel keep throughput below 1 Mb/s under lossy channel conditions as well.

$$
\begin{aligned}
Thr_{\text{ALT}} &= \frac{\text{total \# of bits transmitted successfully}}{\text{total transmission time}} \\
&= \frac{\sum_{i=1}^{n}(1-\phi_i)N_i\ pktL}{\sum_{j=1}^{n}\frac{N_j\ pktL}{R_j}} = \frac{\sum_{i=1}^{n}(1-\phi_i)\alpha_i}{\sum_{j=1}^{n}\frac{\alpha_j}{R_j}} \\
&= \sum_{i=1}^{n}\left[(1-\phi_i)R_i\ \frac{\frac{\alpha_i}{R_i}}{\sum_{j=1}^{n}\frac{\alpha_j}{R_j}}\right] = \sum_{i=1}^{n}(1-\phi_i)R_i\,\overline{\alpha}_i, \qquad (9)
\end{aligned}
$$

where $\overline{\alpha}_i$ denotes the fraction of time spent at R_i.

Using this new metric, we have repeated the simulations for each RAA under corresponding effective jamming strategies. All simulations are run for 100 seconds assuming a perfect channel. The results are given in Table 3.

We observe that effective jamming strategies considered for each RAA are still able to keep the system throughput (as defined in Eq. (9)) below the base rate for default parameter values. Thus, our analysis is verified for both definitions of the throughput metric.

7. Conclusion

In this paper, we introduced a theoretical framework that employs a bursty periodic jamming model and a rate of jamming metric to analyze the vulnerabilities of widely used RAAs. We proved that the jamming rate required to keep throughput performance below the base rate is low for ARF

RAA	**Jammer Parameters**	$\mathbf{Thr}_{\mathrm{ALT}}$
ARF	$a = 1$, $T = 11$	0.952 Mb/s
SampleRate	$a = 44$, $T = 934$	0.994 Mb/s
RARF	$a = 2$, $T = 6$	0.785 Mb/s

Table 3: Throughput values based on Eq. (9) of various RAAs with corresponding effective jamming strategies under a perfect channel

(around 10%), and even lower for SampleRate (around 4%). For ARF, we also proved that bursty periodic jamming is a near-optimal jamming strategy. Thereafter, we proposed a randomized variant of ARF (RARF) and analyzed its performance under the same jamming model.

We proved that one needs a jamming rate of at least 19.5% to keep the throughput of RARF below the base rate. This bound is relatively tight for two-rate RARF. Using ns-3 simulations, we corroborated our analytical results and observed that for IEEE 802.11g, the throughput of RARF falls below the base rate only for RoJ values above 33%, which is more than three times the value required for ARF. The jamming strategies considered can be employed for perfect or lossy channels.

We demonstrated that a randomized approach for adapting transmission rates provides high jamming resistance, without drastically altering average system performance in the absence of jamming. Specifically, a positive feature of RARF is that it does not need to distinguish between legitimate interferers and malicious interferers. As shown, in Fig. 7, in the case of non-adversarial lossy channel conditions, RARF perform similarly to ARF. Thus, with the design of RARF, we showed the added benefit of randomization on the resiliency of a well-known rate control scheme (ARF) against jamming attacks. Although we considered bursty periodic jamming, randomization should be applicable against any jammer that is unaware of the real-time transmission rate.

The analysis in our paper focused on a single pair of node. In the case of multiple pairs of nodes operating within a cell, it is sufficient for an attacker to target a single pair to bring down the throughput of all the pairs, as also noticed in [17]. This is a consequence of the well-known "performance anomaly" problem affecting IEEE 802.11 networks [41].

In summary, our analytical findings and ns-3 simulations show that state-

of-the-art RAAs are vulnerable to jamming attacks that are easy to implement. We propose a solution, leveraging randomization, that is provably more robust as it conceals bit-rate information. Thus, in the future, rate adaptation algorithms should include some level of randomness to increase their resiliency against jamming attacks. We note that a recently proposed RAA, called Minstrel [6], does include some level of randomization, but its behavior is complex. Analysis of Minstrel is an interesting area left for future work. Future work could also aim at deriving a tighter lower bound on the minimum jamming rate for multi-rate RARF, adopting alternative jamming models, investigating the performance of RAAs under general network topologies, and analyzing the case of multiple jammers.

8. Acknowledgements

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

References

[1] JiWire, Global Wi-Fi finder, `http://v4.jiwire.com/`, 2012.

[2] AT&T, Wi-Fi services for stadiums, `http://www.business.att.com/enterprise/online_campaign/wi-fi-stadiums/`, 2011.

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

[4] A. Kamerman, L. Monteban, WaveLAN: A high-performance wireless LAN for the unlicensed band, Bell Labs Technical Journal 2 (1997) 118–133.

[5] M. Lacage, M. H. Manshaei, T. Turletti, IEEE 802.11 rate adaptation: a practical approach, in: Proceedings of the 7th ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems, MSWiM '04, Venice, Italy.

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

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

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

[9] R. Gummadi, D. Wetherall, B. Greenstein, S. Seshan, Understanding and mitigating the impact of RF interference on 802.11 networks, in: Proceedings of the 2007 Conference of the ACM Special Interest Group on Data Communication, SIGCOMM '07, Kyoto, Japan.

[10] M. Wilhelm, I. Martinovic, J. B. Schmitt, V. Lenders, Short paper: reactive jamming in wireless networks: how realistic is the threat?, in: Proceedings of the 4th ACM Conference on Wireless Network Security, WiSec '11, Hamburg, Germany.

[11] W. Xu, W. Trappe, Y. Zhang, T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MOBIHOC '05, Urbana-Champaign, IL, USA.

[12] K. Pelechrinis, M. Iliofotou, S. V. Krishnamurthy, Denial of service attacks in wireless networks: The case of jammers, Communications Surveys & Tutorials, IEEE 13 (2011) 245–257.

[13] B. Zhou, A. Marshall, W. Zhou, K. Yang, A random packet destruction DoS attack for wireless networks, in: Proceedings of the 2008 IEEE International Conference on Communications, ICC '08, Beijing, China.

[14] A. Scott, T. Hardy, R. Martin, R. Thomas, What are the roles of electronic and cyber warfare in cognitive radio security?, in: Proceedings of the 54th IEEE International Midwest Symposium on Circuits and Systems, MWSCAS '11, Seoul, Korea.

[15] W. Chen, Y. Zhang, Y. Wei, The feasibility of launching reduction of quality (RoQ) attacks in 802.11 wireless networks, in: Proceedings of the 14th IEEE International Conference on Parallel and Distributed Systems, ICPADS '08, Melbourne, Victoria, Australia.

[16] A. Kuzmanovic, E. Knightly, Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants, in: Proceedings of SIGCOMM 2003, ACM, pp. 75–86.

[17] G. Noubir, R. Rajaraman, B. Sheng, B. Thapa, On the robustness of IEEE802.11 rate adaptation algorithms against smart jamming, in: Proceedings of the 4th ACM Conference on Wireless Network Security, WiSec '11, Hamburg, Germany.

[18] K. Pelechrinis, I. Broustis, S. V. Krishnamurthy, C. Gkantsidis, ARES: An anti-jamming reinforcement system for 802.11 networks, in: Proceedings of the 2009 ACM Conference on Emerging Networking Experiments and Technology, CoNEXT '09, Rome, Italy.

[19] I. Broustis, K. Pelechrinis, D. Syrivelis, S. V. Krishnamurthy, L. Tassiulas, FIJI: Fighting implicit jamming in 802.11 WLANs, in: Proceedings of the 5th International ICST Conference on Security and Privacy in Communication Networks, SecureComm '09, Athens, Greece.

[20] C. Orakcal, D. Starobinski, Jamming-Resistant Rate Control in IEEE 802.11 WLANs, CISE Technical Report 2011-IR-0021, Boston University, 2011. Also available as `http://www.bu.edu/phpbin/cise/download.php?publication_id=1129`.

[21] J. Kim, S. Kim, S. Choi, D. Qiao, CARA: Collision-aware rate adaptation for IEEE 802.11 WLANs, in: Proceedings of the 25th IEEE International Conference on Computer Communications, INFOCOM '06, Barcelona, Spain.

[22] S. Wong, H. Yang, S. Lu, V. Bharghavan, Robust rate adaptation for 802.11 wireless networks, in: Proceedings of the 12th Annual International Conference on Mobile Computing and Networking, MobiCom '06, Los Angeles, CA, USA.

[23] G. Holland, N. Vaidya, P. Bahl, A rate-adaptive MAC protocol for multihop wireless networks, in: Proceedings of the 7th Annual International Conference on Mobile Computing and Networking, MobiCom '01, Rome, Italy.

[24] M. Vutukuru, H. Balakrishnan, K. Jamieson, Cross-layer wireless bit rate adaptation, in: Proceedings of the 2009 ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, SIGCOMM '09, Barcelona, Spain.

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

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

[27] I. Pefkianakis, Y. Hu, S. Wong, H. Yang, S. Lu, MIMO rate adaptation in 802.11n wireless networks, in: Proceedings of the 16th Annual International Conference on Mobile Computing and Networking, MobiCom '10, Chicago, Illinois, USA.

[28] F. Peng, J. Zhang, W. Ryan, Adaptive modulation and coding for IEEE 802.11n, in: Proceedings of the 2007 IEEE Wireless Communications and Networking Conference, WCNC, Hong Kong.

[29] W. H. Xi, A. Munro, M. Barton, Link adaptation algorithm for the IEEE 802.11n MIMO system, in: Proceedings of the 7th International IFIP-TC6 Networking Conference on Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet, NETWORKING '08, Singapore.

[30] S. Abraham, A. Meylan, S. Nanda, 802.11n MAC design and system performance, in: Proceedings of the 2005 IEEE International Conference on Communications, ICC '05, Seoul, Korea.

[31] C. Chen, H. Luo, E. Seo, N. H. Vaidya, X. Wang, Rate-adaptive framing for interfered wireless networks, in: Proceedings of the 26th IEEE International Conference on Computer Communications, INFOCOM '07, Anchorage, Alaska, USA.

[32] A. Sheth, C. Doerr, D. Grunwald, R. Han, D. Sicker, MOJO: A distributed physical layer anomaly detection system for 802.11 WLANs, in: Proceedings of the 4th International Conference on Mobile Systems, Applications and Services, MobiSys '06, Uppsala, Sweden.

[33] A. G. Fragkiadakis, E. Z. Tragos, T. Tryfonas, I. G. Askoxylakis, Design and performance evaluation of a lightweight wireless early warning intrusion detection prototype, EURASIP J. Wireless Comm. and Networking 2012 (2012) 73.

[34] C. Orakcal, D. Starobinski, Rate adaptation in unlicensed bands under smart jamming attacks, in: Proceedings of the 7th International Conference on Cognitive Radio Oriented Wireless Networks, NSF WiFiUS meeting, CrownCom '12.

[35] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, B. Thapa, On the performance of IEEE 802.11 under jamming, in: Proceedings of the 27th IEEE International Conference on Computer Communications, INFOCOM '08, Phoenix, AZ, USA.

[36] B. Awerbuch, A. Richa, C. Scheideler, A jamming-resistant MAC protocol for single-hop wireless networks, in: Proceedings of the 27th ACM Symposium on Principles of Distributed Computing, PODC '08, Toronto, Canada.

[37] D. Giustiniano, V. Lenders, J. B. Schmitt, M. Spuhler, M. Wilhelm, Detection of reactive jamming in dsss-based wireless networks, in: Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '13, Budapest, Hungary.

[38] SampleRate, MadWifi rate control, `http://madwifi-project.org/browser/madwifi/trunk/ath_rate/sample`, 2011.

[39] D. Bertsimas, J. Tsitsiklis, Introduction to Linear Optimization, Athena Scientific, Nashua, NH, USA, 1997.

[40] ns 3, Network simulator, `http://www.nsnam.org/`, 2012.

[41] M. Heusse, F. Rousseau, G. Berger-Sabbatel, A. Duda, Performance anomaly of 802.11 b, in: INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, volume 2, IEEE, pp. 836–843.

[42] M. Mitzenmacher, E. Upfal, Probability and Computing: Randomized Algorithms and Probabilistic Analysis, Cambridge University Press, New York, NY, USA, 2005.

Appendix A. Proof of Lemma 5

Proving Lemma 5 is equivalent to proving the following inequality:

$$f(x) = \left(1 - \frac{1}{s}\right)^x \frac{e\,x}{s} \leq 1\,, \qquad \text{for } s \geq 2 \text{ and } x \geq 1.$$

Note that $f(x)$ is differentiable for $x \geq 1$. The first order derivative is:

$$f'(x) = e\left(1 - \frac{1}{s}\right)^x \frac{x\,\log\left(1 - \frac{1}{s}\right) + 1}{s}\,.$$

Let $f'(x^\star) = 0$. For $x \geq 1$, the unique solution is:

$$x^\star = -\frac{1}{\log\left(1 - \frac{1}{s}\right)}\,.$$

The second order derivative of $f(x)$ is:

$$f''(x) = e\left(1 - \frac{1}{s}\right)^x \frac{\log\left(1 - \frac{1}{s}\right)}{s}\left[\log\left(1 - \frac{1}{s}\right)x + 2\right].$$

In order to know if $x^\star$ is a maximum or a minimum, we calculate $f''(x^\star)$.

$$f''(x^\star) = \frac{\log\left(1 - \frac{1}{s}\right)}{s} < 0\,, \qquad \text{for } s > 1.$$

Since $f''(x^\star) < 0$, a maximum occurs at $x^\star$. Next, we evaluate $f(x^\star)$, the maximum value of the function $f(x)$ for $x \geq 1$, and show that it is less than or equal to 1:

$$f(x^\star) = -\frac{1}{s\,\log\left(1 - \frac{1}{s}\right)}\,.$$

Since $1 - s^{-1} \leq e^{-s^{-1}}$,

$$\log\left(1 - \frac{1}{s}\right) \leq -\frac{1}{s}\,,$$

leading to $f(x^\star) \leq 1$. Therefore, $f(x)$ is lower than 1 at its maximum point. Since $f(x)$ has only one extreme point, we do not need to check the boundary condition of $x = 1$. Thus, we have proved that $f(x) \leq 1$ for $x \geq 1$ and $s \geq 2$.

Appendix B. Proof of Theorem 3

We begin the proof of Theorem 3 by presenting the following well known bound as given in [42]:

$$1 - z \geq e^{-z-z^2}\ , \quad \text{for } z \in \mathbb{R} \text{ and } z \leq \frac{1}{2}\,. \tag{B.1}$$

We use Theorem 1, Lemma 4 and Eq. (B.1) to obtain a lower bound on the expected throughput as follows:

$$\mathbb{E}[Thr_{\text{RARF}}] \geq \left(\frac{T-f}{T}\right) R_2 - \left[1 - e^{-\frac{s+1}{s^2}(T-f)}\right] \frac{s\,(R_2 - R_1)}{T}\ . \tag{B.2}$$

Now that we have a simplified lower bound expression for the expected throughput, we can obtain an upper bound on the jamming period T, by setting the right-hand side of Eq. (B.2) lower than or equal to R_1.

$$\begin{aligned}
\left(\frac{T-f}{T}\right) R_2 - \left[1 - e^{-\frac{s+1}{s^2}(T-f)}\right] \frac{s\,(R_2 - R_1)}{T} &\leq R_1\ , \\
\left(\frac{R_2}{R_1} - 1\right) \left[T - f - s + se^{-\frac{s+1}{s^2}(T-f)}\right] &\leq f\ , \\
T - f + se^{-\frac{s+1}{s^2}(T-f)} &\leq \frac{f}{\frac{R_2}{R_1} - 1} + s\ .
\end{aligned} \tag{B.3}$$

Let $x = T - f$, and $f(x)$ denote the left side of Eq. (B.3).

$$f(x) = x + se^{-\frac{x(s+1)}{s^2}}.$$

We aim to prove that Eq. (B.3) can be solved for the maximum value of x. We consider $x \geq 1$ since T must always be greater than a for a periodic jammer. First, we show that the inequality is satisfied for $x = 1$.

$$f(1) = 1 + se^{-\frac{s+1}{s^2}} < 1 + s \leq \frac{f}{\frac{R_2}{R_1} - 1} + s,$$

for $R_2 \leq (f+1)R_1$.

Secondly, note that as $x \to \infty$, $f(x) \to \infty$. Lastly, we need to show that $f(x)$ is increasing, i.e. the first order derivative $f'(x)$ is greater than 0, for

$x \geq 1$ to prove that Eq. (B.3) can be solved. The first order derivative of $f(x)$ is as follows:

$$f'(x) = 1 - \left(1 + \frac{1}{s}\right) e^{-\frac{x(s+1)}{s^2}}.$$

Using the well known inequality of $1 + s^{-1} \leq e^{s^{-1}}$ [42],

$$f'(x) \geq 1 - e^{\frac{s-x(s+1)}{s^2}}.$$

For $x \geq 1$, we get $s - x(s+1) < 0$, leading to $e^{\frac{s-x(s+1)}{s^2}} < 1$. Therefore, $f'(x) > 0$ and $f(x)$ is increasing for $x \geq 1$, which enables us to solve Eq. (B.3) for maximum value of T.