Mobile Networks and Applications (2010**) manuscript No.**
(will be inserted by the editor)

Performance of IEEE 802.11 under Jamming

Emrah Bayraktaroglu · Christopher King · Xin Liu · Guevara Noubir · Rajmohan Rajaraman · Bishal Thapa

Received: 15 December 2010 / Accepted:

Abstract We study the performance of the IEEE 802.11 MAC protocol under a range of jammers that covers both channel-oblivious and channel-aware jamming. We consider two channel-oblivious jammers: a *periodic* jammer that jams deterministically at a specified rate, and a *memoryless* jammer whose interfering signals arrive according to a Poisson process. We also develop new models for channel-aware jamming, including a *reactive* jammer that only jams non-colliding transmissions and an *omniscient* jammer that optimally adjusts its strategy according to current states of the participating nodes.

Our study comprises of a theoretical analysis of the saturation throughput of 802.11 under jamming, an extensive simulation study, and a testbed to conduct real world experimentation of jamming IEEE 802.11 using a software defined radio (GNU Radio combined with USRP boards). In our theoretical analysis, we use a discrete-time Markov chain analysis to derive formula for the saturation throughput of 802.11 under memoryless, reactive and omniscient jamming. One of our key results is a characterization of optimal omniscient jamming that establishes a lower bound on the saturation throughput of 802.11 under arbitrary jammer attacks. We validate the theoretical analysis by means of Qualnet simulations. Finally, we measure the real-world performance of periodic, memoryless and reactive jammers using our GNURadio/USRP aided experimentation testbed.

E. Bayraktaroglu · X. Liu · G. Noubir · R. Rajaraman · B.Thapa
College of Computer & Information Science, Northeastern University, Boston MA
E-mail: bthapa@ccs.neu.edu

C. King
Department of Mathematics, Northeastern University, Boston MA
E-mail: king@neu.edu

1 Introduction

[1] The IEEE802.11 CSMA/CA MAC protocol is widely used and operates over many physical layers such as DSSS/FHSS/IR, CCKFHSS (IEEE802.11b), OFDM (IEEE802.11a), and MIMO (IEEE802.11n) [11]. It is reasonably efficient for controlling medium access and delivers a throughput significantly higher than other non-explicit reservation MAC protocols such as Aloha, and variants of CSMA [5]. However, efficiency is achieved through a relatively sophisticated control mechanism, and by making assumptions on the behavior of competing nodes and the characteristics of the channel. Such control mechanisms are usually the target of choice for malicious attackers.

A natural objective of adversaries is to drastically reduce the throughput of the communicating nodes while using as little energy as possible. This can be achieved by carefully jamming critical packets or bits at the right moment, frequency, and location. Such a strategy enables an adversary to devise sophisticated attacks including the partitioning of a network, redirecting traffic through areas under the control of the adversary, or achieving man-in-the-middle attacks. Conserving energy increases the lifetime of jammer nodes (also called cybermines), which then remain a threat for a longer period of time. Building such smart jammers is within the reach of the public at large, due to the availability of low-cost fully controllable Software Defined Radio platforms such as USRP/GNU-Radio [7, 8] and many other partially controllable sensor network platforms operating over the 2.4GHz ISM band [29]. Since IEEE-802.11 MAC is widely used and common to many physical layers, it is important to understand its limits in terms of resiliency to smart jammers.

[1] This work was partially supported by NSF grants 0448330 (CAREER), 0635119, 0915985, and by DARPA under contract HR0011-06-1-0002.

1.1 Our Contributions

In this paper, we study the performance of IEEE802.11 MAC in the presence of various types of jammers through a systematic theoretical analysis, extensive simulations, and a prototype implementation.

- Building on the discrete Markov model of [5], we analyze the saturation throughput of 802.11 (basic mode) under both channel-oblivious and channel-aware jammer models. Our theoretical analysis framework is general and can be used to analyze the resilience of other MAC protocols to jamming.
- We introduce the notion of a channel-aware omniscient jammer and derive key properties of an optimal omniscient jammer. In addition to identifying damaging jamming techniques, our analysis of an optimal jammer provides a lower bound on the throughput achievable by 802.11 under arbitrary adversarial jamming.
- We validate our theoretical analysis through an extensive simulation study using Qualnet. We also develop a GNU-Radio/USRP aided jammer testbed for implementing memoryless,periodic and reactive jammers and compare the prototype results with theory and simulations.
- Our results indicate that while a periodic channel-oblivious jammer is fairly damaging for large packet sizes and large saturated networks, it is significantly less effective than channel-aware jamming, allowing orders of magnitude more throughput for small jamming rates. Furthermore, an optimal omniscient jammer is even 20-30% more effective than other natural channel-aware jammers, and is especially efficient against networks with a small number of active sessions.

1.2 Related Work

Wireless networks are highly sensitive to denial of service attacks. The wireless communication medium is a broadcast channel, exposing the physical layer of wireless communication to jamming originating at arbitrary locations [23, 24]. There has also been considerable research on attacks on the control mechanisms at higher layers as well as cross-layer attacks (e.g., [10,30]). The focus of this paper is on the MAC layer, which is sensitive to attacks targeting the control channels and mechanisms owing to the limited sensing capabilities in the wireless medium [2, 15, 20]. The work [20] analyzes the throughput of CSMA/CA under adversarial jamming, assuming the Poisson arrival of packets. The work of [29] classifies jammer attack models and presents jamming detection techniques.

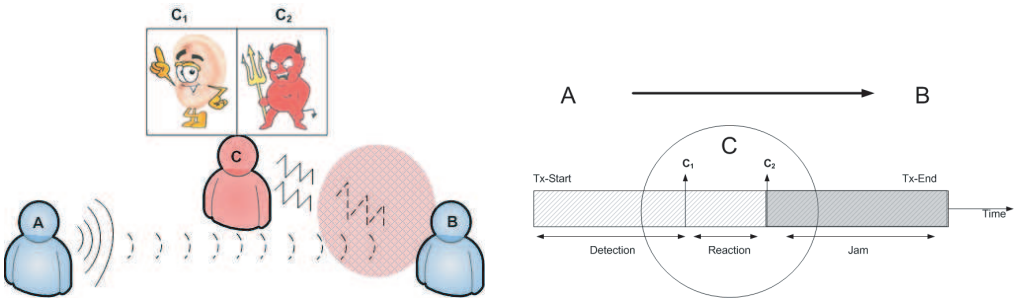
The IEEE 802.11 MAC protocol is widely used and has been extensively analyzed with respect to various performance issues, including throughput, power control, fairness, as well as hidden terminal jamming problems [5, 18, 26]. With the increased ease of building low-cost jammers and increased interest in studying DoS attacks, researchers have started studying the effect of adversarial jamming on 802.11 [2, 17,25]. A recent series of studies analyses the energy-efficiency of several jamming techniques against 802.11 [1, 25]; they demonstrate through extensive simulations that intelligent jamming by concentrating jamming signals on control packets (e.g., CTS or ACK) is significantly more energy-efficient than jammers that are oblivious to the channel. In our work, we have analyzed a wider range of jammers through theoretical analysis, simulations, as well as a GNU radio prototype testbed. Another difference between [1, 25] and our work is that while their performance measure of interest is the jammer energy needed to completely shut down the channel, our study considers the entire throughput range and analyzes how 802.11 throughput varies as a function of jammer rate (and, hence, energy). Another related work studies the impact of periodic jammers on an 802.11 LAN supporting simultaneous Voice over IP (VoIP) connections through simulations [26], while [19] and [16] propose channel hopping and protocol hopping techniques to increase the robustness of 802.11.

Our theoretical contributions build on the framework of [5] for analyzing the saturation throughput of 802.11. There have been several subsequent studies that refine the model of [5] or consider different traffic models, channel conditions, or performance measures (e.g., [6,28]). To the best of our knowledge, our work is the first theoretical analysis of the IEEE 802.11 MAC under adversarial jamming. There has also been considerable interest recently on jamming attacks against sensor networks; [27] gives a taxonomy of attacks, [13] formulates the jammer-network interaction as an optimization problem, while [12] studies the resiliency of several sensor MAC protocols.

2 Models of Communication and Jamming

Medium Access Control Model: IEEE802.11. Our focus is on the IEEE802.11 Distributed Coordination Function (DCF) [11]. DCF is a distributed MAC protocol based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) for networks with or without infrastructure. It has two modes: a basic mode which has a DATA/ACK exchange and an extension with RTS (Request To Send)/CTS (Clear To Send) handshake prior to DATA/ACK. The RTS/CTS exchange was designed to reserve the channel in advance and minimize the impact of collisions but obviously does not help against jamming [1, 25]. In this paper, we only consider the basic mode.

IEEE802.11 defines four types of IFSs (Inter Frame Space): SIFS, DIFS, PIFS, and EIFS [11]. SIFS (Short Interframe Space) is the shortest IFS and is used between RTS, CTS,



(a) Network Setup (b) Timeline Graph

Fig. 1 Block Diagram: A is the sender, B is the receiver, C is the channel-aware jammer (C_1 and C_2 are its sensing and jamming counterparts).

DATA and ACK frames. The PIFS (PCF Interframe Space) is used under PCF (Point Coordination Function) but not in the DCF mode. DCF requires the wireless nodes to defer the transmission until the medium has been idle without interruption for a period of DIFS (DCF Interframe Space) or EIFS (Extended Interframe Space). If the last frame reception is successful, DIFS is applied. If the last frame reception does not result in a correct frame check sequence, EIFS must be applied. In our previous work, we have devised an efficient attack against IEEE802.11 using periodic pulses with a period of EIFS. We have also shown how one can protect against this type of attack [16]. In this paper, we consider DCF without the EIFS functionality. IEEE802.11 uses an exponential backoff scheme for contention avoidance, whose details we defer to Section 3.1, where we present the Markov chain model for our analysis.

Jammer Models for MAC-Layers. We classify jammers of the MAC layer into four abstract categories according to their capability of sensing and reacting to the medium state (*Channel-Oblivious vs. Aware*), and maintaining a state that dictates their future actions (*Memoryless vs. Stateful*):

- **Channel-Oblivious & memoryless** jammers make jamming decisions without sensing the channel, and independently from their past actions. There are only two types of channel-oblivious & memoryless jammers: (a) in continuous time, jamming pulses arrive according to a Poisson distribution; (b) in discrete time, the jammer has a fixed probability of transmitting a pulse every timeslot.
- **Channel-Oblivious & stateful** jammers do not have access to the channel state; however, their actions may be dependent on their past behavior. The simplest example is a *periodic jammer*. A more sophisticated jammer of this type may send a burst of pulses and then stop for a long period of time before repeating. Such a jammer could attempt to drive the nodes into a long backoff period where they do not attempt to send packets even though no jamming is occurring.
- **Channel-Aware & memoryless** jammers have basically one jamming rate for each possible state of the channel (e.g., busy, idle). In a continuous-time model, the pulses are generated according to a Poisson process with different rates for the two states.
- **Channel-Aware & stateful** jammers are the most sophisticated jammers. One such jammer is a *reactive jammer*, which senses the medium and transmits a jamming pulse with a specified probability whenever it detects a non-colliding transmission. The strongest channel-aware and stateful jammer is an *omniscient jammer*, which senses the medium and can identify the number of retransmissions that a packet went through. Whenever such a jammer detects a non-colliding transmission, it transmits a jamming pulse with a probability that may depend on the the backoff stage of the transmitter.

Our paper focuses on four classes of jammers: channel-oblivious & memoryless jammers in continuous time (henceforth abbreviated as *memoryless* jammers), periodic jammers which are a special case of channel-oblivious & stateful jammers, and two channel-aware & stateful jammers: reactive jammers and omniscient jammers.

Figure 1 depicts the network and the adversary model of our system. The adversary depicts the channel-aware jammer. For Channel-Oblivious jammers, the sensing counterpart ($C1$)would be inactive.

3 Theoretical Analysis

Consider a wireless network with n pairs of 802.11 nodes and a jammer that jams the channel at a specified rate. Throughout this section, we make the following assumptions for our analysis: (i) *ideal channel conditions*, that is, any transmission can be heard by every node in the network; thus, there are no hidden terminals or exposed terminals [5]; (ii) *saturation conditions*, that is, every node always has packets to send; and (iii) *ideal jamming conditions*, that is, a jamming signal destroys an 802.11 packet once their transmissions overlap.

Under the above assumptions, we derive the throughput of an 802.11 LAN under three probabilistic jamming models: memoryless, reactive, and omniscient. We derive formu-

lae for the throughput under the three models, and establish key properties of an optimal omniscient jammer. Our characterization of an optimal jammer is, perhaps, the most significant theoretical contribution of this paper. These analyses are developed in Sections 3.2 through 3.4. First, we present an analysis framework that is common to all these jammers.

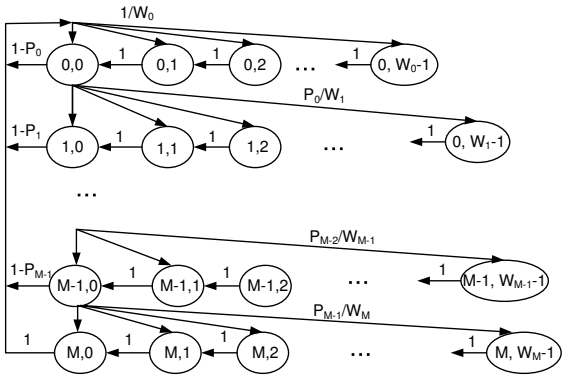


Fig. 2 Markov Chain model under probabilistic jamming

3.1 An Analysis Framework

Following [5], we model the exponential backoff mechanism of 802.11 MAC protocol using a bidirectional discrete-time Markov Chain. Unlike [5], we adopt the protocol standard of a finite retransmission limit (this refinement of [5]'s model has been studied in [28]).

Let $W_0 = CW_{min}$ denote the minimum contention window (CW), W_i be the CW of the ith backoff stage and M be the maximum retransmission limit. CW doubles when a transmission fails, i.e. $W_i = 2^i W_0$, until it reaches the maximum contention window CW_{max}. If the number of retransmissions exceeds M, the sender discards the current packet in the queue and resets CW to W_0. Note that if $M > \log_2 \frac{CW_{max}}{CW_{min}}$, the last several backoff stages stay constant at CW_{max}. For simplicity, we will assume for our analysis that $M = \log_2 \frac{CW_{max}}{CW_{min}}$.

Figure 2 depicts the state transition of one 802.11 node in a discrete-time Markov chain. The communication is divided into *timeslots*. At the beginning of each timeslot, the backoff counter decreases by one, as shown in the figure, and the node transits from state (i, j) to state $(i, j-1)$. When the backoff counter reaches zero, the node initiates a transmission. If the transmission succeeds, the node resets its backoff stage and enters $(0, j)$, where j is chosen uniformly at random from $[0, W_0 - 1]$. Otherwise, the node doubles its CW and enters state $(i + 1, j)$, where j is chosen uniformly at random from $(0, W_{i+1} - 1)$. We note that the amount of time that a node spends in a state (the length of a timeslot), is variable, depending on whether the channel is busy (owing to an ongoing transmission, or even a jamming signal) or the channel is idle (in which case it equals the 802.11 physical slot parameter σ).

There are two reasons for the failure of a packet transmission by a node (which happens in a state of the form $(i, 0)$): the packet collides with a packet transmission initiated by another node, or the packet (or the associated ACK) is jammed by the jammer. We follow one fundamental assumption in Bianchi's model that in steady state, the probability that a packet transmission collides with a packet transmitted by another 802.11 node is independent of the current state of the transmitting node [5]. This assumption is justified, especially for a sufficiently large number of nodes and sufficiently large contention window size. Let P_c denote this collision probability.

Each of the three jammers we analyze in this section are probabilistic jammers, and can be captured by the probability with which they jam the channel at a given time. For the memoryless jammer, this probability is constant, independent of the state of the nodes. A reactive jammer, on the other hand, jams only when a transmission is ongoing and there are no collisions, but the jamming probability is independent of the backoff stage. Finally, the jamming probability of an omniscient jammer may depend on the backoff stage of the transmitting node. We define the *jamming probability* q_i of a jammer to be the probability of jamming an ongoing transmission in state $(i, 0)$ *conditioned on the event that there is no collision with another 802.11 transmission*. We now obtain that P_i, the probability that a transmission in backoff stage i fails, is given by $P_i = P_c + (1 - P_c)q_i$.

We are now ready to derive the state occupancy probabilities, which follow using standard Markov chain techniques. Let $b_{i,j}$ denote the probability for a node to be in the backoff stage i with backoff counter equals j in a steady state. We formulate the state transitions by following set of equations.

$$b_{i,j} = \begin{cases} b_{i,j+1} + P_i b_{i-1,0}/W_i & i > 0, j < W_i - 1 \\ P_i b_{i-1,0}/W_i & i > 0, j = W_i - 1 \neq 0 \\ b_{0,j+1} + b_{M,0}/W_0 & i = 0, j < W_0 - 1 \\ b_{M,0}/W_0 & i = 0, j = W_0 - 1 \end{cases}$$

Given values for the failure probabilities P_i, the above equations, together with the normalization condition that the $b_{i,j}$'s sum to one, can be solved to obtain the $b_{i,j}$ values. Since each node transmits only when its backoff counter reaches zero, the steady state transmission probability τ is given by $\sum_{i=0}^{M} b_{i,0}$. Given τ, P_i, and the protocol-related parameters packet length L, header size H, acknowledgment length ACK, we compute the throughput by determining the channel time-wise utilization for successful payload transmissions. The normalized throughput Γ is expressed by

(1) [5].

$$\Gamma = \frac{E[\text{Payload transmitted in a timeslot}]}{E[\text{length of a timeslot}]} \quad (1)$$

The numerator of the above equation equals $P_s L$, where P_s is the probability that there is a successful transmission in a given timeslot (this depends on τ and the P_i's, and the particular jammer model), and L is the duration of the payload of a packet. The denominator of Equation 1 is given by

$$E[\text{length of a timeslot}] = P_{tr}T_{tr} + (1 - P_{tr})T_{id},$$

where $P_{tr} = 1 - (1 - \tau)^n$ is the probability that at least one node transmits in a given timeslot, T_{tr} is the time taken by a timeslot during which a transmission occurs, and T_{id} is the time taken by an idle timeslot (when no 802.11 node transmits). Specifying τ, P_s, T_{tr} and T_{id} then yields the throughput using (1). Finally, we define the rate of a jammer to be simply the fraction of time it jams the channel; it lies in $[0, 1]$. For example, a periodic jammer that emits pulses of width 1 μs every ms has a rate of $1/1000$, and a continuous jammer has rate 1.

3.2 Memoryless Jammers

A memoryless jammer generates jamming signals such that the idle time between successive signals is drawn from an exponential distribution specified by the jamming pulse rate R, which is defined as the number of jamming pulses that the jammer generates per second. The probability that a jamming signal is generated during a time interval t_0 is $(1 - e^{-Rt_0})$; this is, indeed, the jamming probability q_i for all i. Since q_i is independent of i, the failure probability P_i is also independent of i; let p denote this common failure probability. We obtain that

$$p = P_c + (1 - P_c)(1 - e^{-R(\text{DATA+ACK})}),$$

where DATA and ACK refer to the duration of a data and ACK packet, respectively. The DATA term includes both payload length L as well as any headers.

Following our framework of Section 3.1, we now derive the throughput by specifying τ, P_s, T_{tr}, and T_{id}. Plugging in the failure probability into the b_{ij} equations, we get:

$$b_{0,0} = \frac{2(1 - 2p)(1 - p)}{(1 - p)(1 - (2p)^{M+1})W + (1 - 2p)(1 - p^{M+1})} \quad (2)$$

The steady state transmission probability τ is given by

$$\tau = \frac{2(1 - 2p)(1 - p^{M+1})}{(1 - p)(1 - (2p)^{M+1})W + (1 - 2p)(1 - p^{M+1})} \quad (3)$$

Solving (2), (3), and the equation $P_c = 1 - (1 - \tau)^{n-1}$ over the three unknowns τ, p, and P_c yields τ.

We now determine P_s, T_{tr}, and T_{id}.

$$P_s = n\tau(1 - \tau)^{n-1}e^{-R(\text{DATA+ACK})}$$
$$T_{tr} = \text{DIFS} + \text{SIFS} + \text{DATA} + \text{ACK}$$
$$T_{id} = (1 - e^{-R\sigma})\sigma + (1 - e^{-R\sigma})(\text{EDIFS} + \sigma + w),$$

where EDIFS is the expected time before a DIFS period occurs without a jamming pulse. This can be calculated using standard formulae for the exponential model. The above equations in conjunction with the equations of Section 3.1 give us the throughput of the system. The rate of a memoryless jammer with pulse rate R and pulse width w seconds is simply wR. We note that the above analysis assumes that the pulse width of the jammer exceeds the Clear Channel Assesment (CCA) length, hence the nontrivial calculation for T_{id}. If the pulse width is smaller than CCA, then the above equations can be simplified.

3.3 Reactive Jammers

We specify a reactive jammer by its jamming probability q, which is the probability that the jammer jams an ongoing packet transmission that has not undergone a collision.

Since the jamming probability is independent of the backoff stage, the failure probability is also constant for all backoff stages. Let this probability be p. We obtain:

$$p = P_c + (1 - P_c)q \quad (4)$$

The steady state transmission probability τ is given by the same equation (3). Solving (4), (3), and $P_c = 1-(1-\tau)^{n-1}$ yields τ. The probability of success of a given transmission, P_s, is given by $P_s = n\tau(1 - \tau)^{n-1}(1 - q)$, while T_{tr} and T_{id} are DIFS + SIFS + DATA + ACK and σ, respectively.

The above equations in conjunction with Equations of Section 3.1 give us the throughput of the system. The rate of a reactive jammer with jamming probability q is given by

$$R = \frac{qn\tau(1 - \tau)^{n-1}w}{E[\text{length of a timeslot}]},$$

where w is the length of a jamming pulse.

3.4 Omniscient Jammers

In this section, we analyze an omniscient jammer that is aware of the current state of each 802.11 node and adopts a jamming strategy that minimizes system throughput subject to constraints on the jamming rate. While a completely omniscient jammer may not be realizable in practice, effective approximations can be implemented (see Sec 6 for brief discussion). An accurate analysis of omniscient jammers would provide a useful lower bound on the system throughput of 802.11 against all jammers and a measure

for MAC resiliency. Here, we provide a partial analysis of an omniscient jammer, proving interesting properties of an optimal omniscient jammer and characterize certain special cases.

We first make several observations about an optimal omniscient jammer: (a) An optimal omniscient jammer only jams the channel when a transmission of an ACK occurs. (b) An optimal omniscient jammer jams an ongoing transmission only if it incurs no collision. (c) When a transmission is ongoing, the probability with which an optimal omniscient jammer jams the transmission is independent of the particular nodes involved in the transmission. We omit a formal proof of the above three claims owing to space constraints.

3.4.1 Throughput calculation

We model an omniscient jammer by a *jamming vector* $\mathbf{q} = (q_0, q_1, q_2, \ldots, q_M)$, where q_i is the probability that the jammer jams an ongoing transmission of a node in the ith backoff stage, conditioned on the fact that there is no collision. Given the jamming vector $\mathbf{q}$, the throughput of the system and the rate of the jammer can be calculated using the framework of Section 3.1.

The failure probability P_i is given by $P_c + (1 - P_c)q_i$ and the product P_s is given by

$$P_i = n \sum_{i=0}^{M} b_{i,0}(1 - P_c)(1 - q_i) \tag{5}$$

The times T_{tr} and T_{id} are DIFS + SIFS + DATA + ACK and σ, respectively. Since the expected length of a timeslot equals $(1 - (1 - \tau)^n)T_{tr} + (1 - \tau)^n\sigma$, the normalized throughput of the system equals

$$\mathit{\Gamma} = \frac{nL \sum_{i=0}^{M} b_{i,0}(1 - P_c)(1 - q_i)}{(1 - (1 - \tau)^n)T_{tr} + (1 - \tau)^n\sigma}$$

The rate of an omniscient jammer with jamming vector $\mathbf{q}$ is

$$R = \frac{nw \sum_{i=0}^{M} b_{i,0}(1 - P_c)q_i}{(1 - (1 - \tau)^n)T_{tr} + (1 - \tau)^n\sigma},$$

where w is the length of a jamming pulse. The above two equations can be combined to yield

$$\mathit{\Gamma} = \frac{nL(1 - P_c)\tau}{(1 - (1 - \tau)^n)T_{tr} + (1 - \tau)^n\sigma} - \frac{LR}{w} \tag{6}$$

In the remainder of this section, we analyze *optimal* rate-constrained omniscient jammers. For convenience, we represent all times as a multiple of σ, and replace T_{tr} by T and σ by 1.

3.4.2 Properties of an optimal omniscient jammer

Let R denote the rate at which an optimal jammer is jamming the channel. The optimal jammer, constrained by jamming rate R, aims to minimize the total throughput, and is specified by the solution to the following optimization problem

$$\text{minimize} \quad \frac{Ln(1-P_c)\tau}{(1-(1-\tau)^n)T_{tr}+(1-\tau)^n\sigma} - \frac{LR}{w} \tag{7}$$

$$\text{subject to} \quad \sum_{i=0}^{M} \frac{nwb_{i,0}(1-P_c)q_i}{(1-(1-\tau)^n)T_{tr}+(1-\tau)^n\sigma} = R \tag{8}$$

The above optimization problem is a complex non-linear program and does not appear to admit a closed-form solution. Our analysis here is largely guided by numerical calculations and simulations that we have performed (discussed in detail in Section 4).

For the purposes of analysis, we focus our attention on the effect of the jammer on a single node N. Towards this end, we separate out the transmission probability of N as τ_0, letting τ be the common transmission probability of other nodes.

Lemma 1 *For a fixed jammer rate R and collision probability P_c, the throughput $\mathit{\Gamma}$ is a monotonic function of τ_0; i.e., the sign of the partial derivative $\partial\mathit{\Gamma}/\partial\tau_0$ is independent of τ_0.*

Proof Expressed as a function of τ_0, the throughput $\mathit{\Gamma}$ of the system is given by

$$\frac{L(1 - P_c)(\tau_0 + (n - 1)\tau}{(1 - (1 - \tau)^{n-1}(1 - \tau_0))T_{tr} + (1 - \tau)^{n-1}(1 - \tau_0)\sigma} - \frac{LR}{w}$$

where τ is the transmission probability of any node and R is the jammer rate. Since $\mathit{\Gamma}$ is of the form $(A\tau_0 + B)/(C\tau_0 + D) + E$ for some terms A, B, C, D, and E, independent of τ_0, we obtain that $\partial\mathit{\Gamma}/\partial\tau_0$ equals $(AD - BC)/(C\tau_0 + D)^2$, whose sign is independent of τ_0, completing our proof.

We next present the main theorem of this section, which provides a key characterization of an optimal jamming vector, for a given jamming rate and fixed collision probability. We conjecture that the claim of the theorem holds even when the collision probability is allowed to vary according to our original model (and Bianchi's). All of our numerical calculations and simulations support this conjecture; however, we are unable to prove it at this time.

Theorem 1 *For any achievable rate R, assuming a fixed collision probability P_c, there exists an optimal omniscient jammer with rate R which satisfies the following condition: there exists at most one i, $0 \leq i \leq M$, such that q_i lies in the open interval $(0, 1)$.*

Proof Consider an optimal jammer's actions against node N, while keeping the jammer's actions against other nodes fixed. Suppose the jammer is defined by a vector $\mathbf{q}$ in which q_i and q_j are both in $(0,1)$. We will analyze the impact of the jammer changing the jamming probabilities q_i and q_j for N while maintaining all other jamming probabilities the same as in $\mathbf{q}$; i.e., the jamming probabilities remain the same for all levels against other nodes, and for all levels $\neq i,j$ against node N. We will prove that q_i and q_j can be changed continuously (for node N) without increasing the throughput of the system and without changing the total jamming rate R, eventually ending up with two new values, one of which is either 0 or 1. Repeating this argument for all other fractional pairs, and for all nodes, will imply that the optimal strategy can be achieved with values where at most one of the q_i is in $(0,1)$.

Suppose that q_i and q_j are fractional, with $i < j$, and define for convenience

$$x = p_i = P_c + (1-P_c)q_i, y = p_j = P_c + (1-P_c)q_j \quad (9)$$

The pair (x,y) lies in the square $[P_c,1] \times [P_c,1]$, since $0 \leq q_i, q_j \leq 1$. We will write $\tau_0(x,y)$ for the transmission probability of N, ignoring the dependence of τ_0 on the other jamming rates q_k which are held constant throughout. In order to keep the total jamming rate R constant we cannot vary x and y independently. The constraint that R is fixed implies a relation between x and y, which we will determine shortly (20). The relation (20) can be solved to give y as a function of x in the interval $[P_c,1]$, and so the constrained transmission probability is $\tau(x,y(x))$.

By Lemma 1, the throughput is a monotonic function of τ_0. We note that the transmission probabilities of all other nodes remain fixed. So the relevant question is to determine how τ_0 varies as a function of the jamming probabilities at each level. We will compute the derivative

$$\frac{d}{dx}\,\tau_0(x,y(x)) \quad (10)$$

and show that either it is identically zero, or else is never zero.

In the first case where (10) is zero, it follows that τ_0 is constant along the curve $(x,y(x))$. The graph $(x,y(x))$ intersects the boundary of $[P_c,1] \times [P_c,1]$ at two points. At these points one or both of q_i, q_j is 0 or 1. Therefore by choosing these values in place of the original ones we can reduce the number of fractional values among the jamming probabilities without changing R or τ_0, and hence Γ, as claimed.

In the second case where (10) is never zero, it follows that τ_0 is strictly monotone along the curve $(x,y(x))$. Since the sign of $\partial\Gamma/\partial\tau_0$ is independent of τ_0, Γ is smaller at one of the points where this curve intersects the boundary of the square. By choosing the values of q_i, q_j at this point we again reduce the number of fractional values without increasing Γ or R.

It remains to derive the relation (20) and compute the derivative (10). To simplify notation define

$$\gamma_0 = 1, \quad \gamma_k = \prod_{l=0}^{k-1} P_l \;\; k = 1,\ldots,M \quad (11)$$

where P_l is the probability of a failed transmission at level l. We then have $b_{k,0} = b_{0,0}\gamma_k$ for $i = k,\ldots,M$, and from the normalization condition we deduce

$$b_{0,0}^{-1} = \sum_{k=0}^{M} \gamma_k W_k \quad (12)$$

where $W_k = (2^k W + 1)/2$. Note that γ_k does not depend on x or y for $k \leq i$, so the right side of (12) can be written

$$b_{0,0}^{-1} = A + \sum_{k=i+1}^{M} \gamma_k W_k \quad (13)$$

where A is a constant. Now γ_k is a linear function of $x = p_i$ for all $k \geq i+1$, so we can write (13) as

$$b_{0,0}^{-1} = A + xB + \sum_{k=j+1}^{M} \gamma_k W_k \quad (14)$$

with another constant B. Finally γ_k is also a linear function of $y = p_j$ for all $k \geq j+1$, so we end up with the expression

$$b_{0,0}^{-1} = A + xB + xyC \quad (15)$$

with a third constant C. We now consider τ_0:

$$\tau_0 = \sum_{k=0}^{M} b_{k,0} = b_{0,0} \sum_{k=0}^{M} \gamma_k \quad (16)$$

By applying the same reasoning we get the expression

$$\tau_0 = b_{0,0}(H + xJ + xyK) \quad (17)$$

Separating out the jamming component against node N from that against other nodes, we can write the jamming rate R as

$$\frac{(1-P_c)w\sum_{k=0}^{M} b_{k,0}q_k + D}{(1-(1-\tau)^{n-1}(1-\tau_0))T_{tr} + (1-\tau)^{n-1}(1-\tau_0)\sigma}, \quad (18)$$

where D is a constant (since the jamming probabilities against nodes other than N remain the same). Since $(1-P_c)q_k = p_k - P_c$, we can apply similar reasoning on the right side of (18) to end up with the expression for R

$$\frac{b_{0,0}\,(E + xF + xyG)}{(1-(1-\tau)^{n-1}(1-\tau_0))T_{tr} + (1-\tau)^{n-1}(1-\tau_0)\sigma} \quad (19)$$

where E, F, G are again constants. The denominator of (19) is of the form $\alpha\tau_0 + \beta$ for constants α and β. Combining (15), (17), and (19) yields the desired relation between x and y:

$$axy = bx + c \quad (20)$$

where a, b, c are constants. Assuming that $a \neq 0$ the solution $y(x)$ of (20) is defined for all x in $[P_c, 1]$, as claimed (we will consider the case where $a = 0$ at the end). Combining (17) with (15) and using (20) to remove the terms with xy we get

$$\tau_0 = \frac{c_1 + c_2 x}{c_3 + c_4 x} \tag{21}$$

for some constants c_i. The derivative with respect to x is

$$\frac{d}{dx}\tau_0 = \frac{c_2 c_3 - c_1 c_4}{(c_3 + c_4 x)^2} \tag{22}$$

Therefore the derivative is either identically zero (if $c_2 c_3 = c_1 c_4$) or else is never zero, as claimed.

Finally if $a = 0$ in (20) then y can be freely varied in (17) without changing R, and its derivative with respect to y is either identically zero or never zero. Therefore the value of τ_0 is minimized at either $q_j = 0$ or $q_j = 1$.

Intuitively, this suggests that an optimal jammer assigns a certain priority order to the backoff stages of the node N, completely jamming transmissions made at a certain backoff stage before jamming transmissions made at a different stage. Our experiments indicate that this is indeed the case. It turns out, however, that this priority order among the backoff stages may depend in subtle ways on the number of nodes n, L (and, thus, T_{tr}), and P_c. We have been able to establish tight characterizations for two important subcases, when $n = 1$, and when the packet sizes are small.

Theorem 2 *For $n = 1$, an optimal jamming vector is $(q, 1, 1, \ldots, 1, 0)$ or of the form $(1, 1, \ldots, 1, q)$.*

Proof When $n = 1$, $P_c = 0$. So, for any positive jamming rate R, $q_0 > 0$. Furthermore, if q_i is zero for some i, we can assume without loss of generality that q_j, for $j > i$, are all zero since the node will never reach backoff stage $i + 1$ or higher.

We first show that $q_M \leq q_i$, for all $i < M$. The proof is by contradiction. Suppose there exists an optimal jammer for which there is an i such that $q_i < q_M$. We can keep the jammer rate fixed by increasing q_i and decreasing q_M appropriately. It is easy to see that τ is unaffected by a change to q_M; on the other hand, it decreases when q_i increases. By (6), when $n = 1$, Γ is a monotonically increasing function of τ, so we obtain that for an optimal jammer, $q_i \geq q_M$ for all $i < M$.

We next show that if $q_0 = q \in (0, 1)$, then $q_i = 1$ for $0 < i < M$. If the claim is not true, then there exists an $i \in [1, M - 1]$ such that $q_i \neq 1$. Let k be the smallest such i. By Theorem 1, this implies that $q_i = 0$. We now consider an alternative jamming vector that is identical to $\mathbf{q}$ except that the jamming probability is q^* (to be specified shortly) at level 0 and 1 at level i. We set q^* such that the expected time to return to backoff stage 0 is the same under both vectors.That is,

$$q(\sum_{i=0}^{k}(W_i + 1)/2 + k(T - 1)) + (1 - q)((W_0 + 1)/2 + T - 1) =$$
$$q^*(\sum_{i=0}^{k+1}(W_i + 1)/2 + (k + 1)(T - 1)) + (1 - q)((W_0 + 1)/2 + T - 1)$$

This yields

$$\frac{q*}{q} = \frac{\sum_{i=1}^{k}(W_i + 1)/2 + k(T - 1)}{\sum_{i=1}^{k+1}(W_i + 1)/2 + (k + 1)(T - 1)} \tag{23}$$

(Here we use T to denote T_{tr}/σ.) In each case, every packet is eventually successfully transmitted, so the throughput is identical under both jamming vectors. On the other hand, the ratio of the rate of $\mathbf{q^*}$ and that of $\mathbf{q}$ is $(k + 1)q^*/(kq)$, which by (23) and the fact that $W_i = 2^i W_0$, is at most one, completing the proof of this case.

The remaining case is when $q_0 = 1$. In this case, we prove that if there exists $i < M$ such that $q_{i-1} = 1$ and $q_i = q \in (0, 1)$, we can set q_i to to 1 and q_{i-1} to a suitably chosen q^* without increasing either the throughput or the jammer rate. The argument is similar to the above. Again, we choose q^* such that the expected time to return to backoff stage 0 is identical for both jamming vectors. In particular,

$$q^* = \frac{(W_i + 1)/2 + q(W_{i+1}/2 + 1/2)}{W_i/2 + W_{i+1}/2 + 1}.$$

The difference between the jamming rate of the new vector and that of the old one is proportional to

$$2q^* - q - 1 = (W_{i+1} - W_i)(q - 1)/2 \leq 0,$$

establishing the desired claim and completing the proof.

Second, we have studied the case where the packet size is very small, so we can assume that T_{tr} is close to the slot length σ.

Theorem 3 *If $T_{tr} = \sigma$ and $P_c \leq 0.5$, the jamming vector of an optimal omniscient jammer satisfies the following conditions: $q_i \leq q_{i+1}$, for $0 \leq i < M - 1$, and $q_M \leq q_0$.*

Proof As in the proof of Theorem 1, we will focus our attention on an optimal jammer's actions against an individual node N, while keeping the jammers effect on other nodes fixed. Let τ_0 denote the transmission probability of the node N, and let $\mathbf{q}$ denote the jamming vector. For $T = 1$, we first establish that $q_M \leq q_i$, for all $i < M$. This part of the proof is similar to that in Theorem 2. Suppose there exists an optimal jammer for which there is an i such that $q_i < q_M$.

We can keep the jammer rate fixed by increasing q_i and decreasing q_M appropriately. It is easy to see that τ_0 is unaffected by a change to q_M; on the other hand, it decreases when q_i increases. Since Γ is an increasing function of τ_0 for $T = 1$, we obtain that for an optimal jammer, $q_i \geq q_M$ for all $i < M$.

The remainder of the proof is also by contradiction. Let i be the largest index such that $q_i > q_{i+1}$. By the above claim and Theorem 1, we now have one of two cases: $q_i = q \in (0, 1)$ and $q_{i+1} = 0$, or $q_i = 1$ and $q_{i+1} = q \in (0, 1)$, for some q.

We first consider the case where $q_i = q \in (0, 1)$ and $q_{i+1} = 0$. In this case, the expected number of timeslots that node N is in backoff stage i or higher before returning to backoff stage 0 is

$$W_i + (P_c + (1 - P_c)q)W_{i+1} + P_c(P_c + (1 - P_c)q)L_{i+2}, \quad (24)$$

where L_{i+2} is the expected number of timeslots that N is backoff stage $i + 2$ or higher before returning to backoff stage 0.

We now argue that if q is sufficiently large then a different jamming vector $\mathbf{q^*}$, given by $(q_0, q_1, \ldots, q^*, 1, q_{i+2}, \ldots)$ achieves a lower throughput with a lesser jamming rate, for a suitably chosen q^*. We divide the first case into two subcases: $q \geq P_c k/(1 + P_c k)$ and $q < P_c k/(1 + P_c k)$, where $k = L_{i+2}/W_{i+1}$.

We consider the first subcase. The expected number of timeslots that node N is in backoff stage i or higher before returning to backoff stage 0, under the q^*-vector is

$$W_i + (P_c + (1 - P_c)q^*)W_{i+1} + (P_c + (1 - P_c)q^*)L_{i+2}, \quad (25)$$

We set q^* so that the two terms in Equations 24 and 29 are equal.

$$q^* = \frac{qW_{i+1} - P_c(1 - q)L_{i+2}}{W_{i+1} + L_{i+2}} \quad (26)$$

Note that (26) is valid (i.e., $q^* \leq 1$) since q is at least $P_c k/(1 + P_c k)$.

We now argue that the throughput under the jammer $\mathbf{q}$ is at least as high as the throughput under the jammer $\mathbf{q^*}$. The probability that we have a successful transmission once we enter backoff stage i, under the q jamming vector, is

$$(1 - P_c)(1 - q) + (P_c + (1 - P_c)q)(1 - P_c) + P_c(P_c + (1 - P_c)q)P \geq 1 - P_c + P_c P,$$

where P is the probability that we have a successful transmission conditioned on the event that we enter backoff stage $i + 2$. On the other hand, the probability that we have a successful transmission once we enter backoff stage i, under $\mathbf{q^*}$, is

$$(1 - P_c)(1 - q^*) + (P_c + (1 - P_c)q^*)P \leq 1 - P_c + P_c P.$$

To complete the analysis for this subcase, we need to show that the jamming rate of $\mathbf{q^*}$ is at most that of $\mathbf{q}$. Let the number of jamming pulses of the two vectors, conditioned on the event that N enters backoff stage $i + 2$, be r'. Then, the number of jamming pulses of the q-vector, conditioned on the event that N enters backoff stage i, equals

$$m = (1 - P_c)q + (P_c + (1 - P_c)q) \cdot P_c \cdot r',$$

while the number of jamming pulses of $\mathbf{q^*}$, conditioned on the event that N enters backoff stage i, equals

$$m^* = (1 - P_c)q^* + (P_c + (1 - P_c)q^*)(1 - P_c) + (P_c + (1 - P_c)q^*) \cdot r'$$

Elementary algebraic manipulation shows that we can establish $m^* \leq m$ by showing the following inequality.

$$q^* \leq \frac{q - P_c + r' P_c(q - 1)}{2 - P_c + r'} \quad (27)$$

We now compare Equations 26 and 27. We use k to denote L_{i+2}/W_{i+1} for convenience. We note that $r' \leq k/4$ since q_{i+2} is zero by the choice of i and the fact that the window sizes grow exponentially. Since $P_c \geq 0$ and $k \geq 2$, we obtain that $2 - P_c + r' \leq 1 + k$. Since $r' \leq k$ and $q \leq 1$, Equation 27 follows from Equation 26 if $q/(1+k) \leq (q - P_c)/(2 - P_c + r')$. Since $q \geq P_c k/(1 + P_c k)$ and $r' \leq k/4$, we obtain that the desired inequality holds for $P_c \leq 1/2$.

We now consider the second subcase of the first case: $q < P_c k/(1 + P_c k)$. We now argue that a different jamming vector $\mathbf{q^*}$, given by $(q_0, q_1, \ldots, q_{i-1} 0, q^*, q_{i+2}, \ldots)$ will outperform the jammer given by $\mathbf{q}$; that is, it will reduce the throughput without increasing the rate. Our analysis approach will the same as above. That is, we set Q^* such that the expected number of timeslots that node N spends in stage i and above before returning to stage 0, is identical under the two jamming vectors.

The expected number L^* of timeslots that node N is in backoff stage i or higher before returning to backoff stage 0, under the $\mathbf{q^*}$ is

$$W_i + P_c W_{i+1} + P_c(P_c + (1 - P_c)q^*)L_{i+2}$$

Equating the expressions in Equations 24 and 28, we obtain

$$q^* = q\frac{1 + P_c k}{P_c k},$$

which is a valid value for q^* since q is upper bounded by $P_c k/(1 + P_c k)$.

Since $q^* > q$, the throughput achieved under the $\mathbf{q^*}$-vector is at most that under $\mathbf{q}$. It now remains to prove that the jamming rate of $\mathbf{q^*}$ is at most that of the $\mathbf{q}$. The number of jamming pulses under $\mathbf{q^*}$, conditioned on node N entering backoff stage i, is equal to

$$P_c(1 - P_c)q^* + P_c(P_c + (1 - P_c)q^*)r',$$

which is true if $P_c \leq (k - r' - 1)/k$. The preceding inequality follows from $P_c \leq 1/2$ by using the fact that either $k = 2$ and $r' = 0$ or $k \geq 2 + 4(1 - P_c)$ and $r' \leq k/4$.

We finally consider the second case $q_i = 1$ and $q_{i+1} = q \in (0, 1)$, for some q. Our argument follows a similar approach as for the first case. We argue that the jamming vector $\mathbf{q^*}$, given by $(q_0, q_1, \ldots, q_{i-1}, q^*, 1, q_{i+2}, \ldots, q_M)$, will result in no larger throughput using a smaller jamming rate. We first set q^* such that expected number of timeslots that node N spends in backoff stages i and greater, conditioned on the event that it enters backoff stage i, is equal for the two jamming vectors. This is obtained by setting q^* such that

$$W_i + W_{i+1} + (P_c + (1 - P_c)q)L_{i+2} = W_i + (P_c + (1 - P_c)q^*)(W_{i+1} + L_{i+2}).$$

This yields

$$q^* = \frac{1 + qk}{1 + k},$$

where k is defined as before. We note that since $q \leq 1$, $q^* \geq q$. This immediately implies that the throughput under $\mathbf{q^*}$ is no more than that under $\mathbf{q}$.

We finally argue that the jamming rate of $\mathbf{q^*}$ is at most that of $\mathbf{q}$. The expected number of jamming pulses transmitted under $\mathbf{q}$, conditioned on the event that node N enters stage i is

$$(1 - P_c) + (1 - P_c)q + (P_c + (1 - P_c)q) \cdot r' \quad (28)$$

while the expected number of jamming pulses transmitted under $\mathbf{q^*}$, conditioned on the event that node N enters stage i is

$$(1 - P_c)q^* + (P_c + (1 - P_c)q^*)(1 - P_c + r') \quad (29)$$

where r' is the expected number of jamming pulses under either of the two vectors, conditioned on the event that node N enters stage $i + 2$. The expression in Equation 29 is at most that in Equation 28 if

$$q^* \leq \frac{1 - P_c + q(1 + r')}{1 - P_c + (1 + r')}.$$

Since $q^* = (1+qk)/(1+k)$, $P_c \leq 1/2$ and $1+r' \leq k/2$, the above inequality holds, completing the proof of the second case and, thus, the proof of the theorem.

4 Simulation Evaluation

In this section, we validate our theoretical analysis for memoryless, reactive and omniscient jamming models by an extensive simulation study. We investigate and compare the performance of these three jammers and an additional periodic jammer in terms of their efficiency in reducing network throughput under various network setup.

Setup: We run our experiments on the Qualnet 3.9.5 simulator [21]. We set up a 1Mbps IEEE802.11 network that satisfies the ideal channel and jamming conditions, and the saturation scenario, discussed in Section 3. Towards this end, we locate n sender-receiver pairs in a 300 $\times$ 300 m^2 area for varying n, and set their transmission powers to 10dBm so that they can hear one another. Each sender has an unbounded queue of packets. We run IEEE802.11 DCF in the basic model with EIFS disabled.

We implement the memoryless and periodic jammers by attaching an exponential and periodic traffic generator, respectively to an independent node. We emulate the reactive and omniscient jammers by dropping the packets according to the jamming probability of the associated jammer. The jamming vector (jamming probabilities at each stage) of the omniscient jammer is set by solving the optimization problem (8) for given jamming rates using Maple Software. In all of our simulation runs, the jammer is located next to the receiver and the jamming pulse width is set to be $22\mu s$. This value is empirically chosen as it is found to be the smallest pulse width sufficient enough to destroy the packet, if hit, at the receiver side but without disturbing the sender.

Results:

1. We first take a look at the performance of memoryless jammer for various packet sized network. Figure 3 shows the throughput of a session with packet sizes varying from 100 bytes to 1500 bytes under three different jamming rates. As we can see the graph, simulation results match the theoretical results pretty well. The figure also indicates that there exists a performance trade-off between packet size and throughput for a given jamming rate. Large packet sizes incur less overhead and yield higher throughput in the absence of jamming. However, larger packets are more susceptible to jamming when the jamming rate is high, and thus smaller packet sizes yield higher throughput in the presence of jamming. .
2. Second, we look at the analysis of memoryless jamming with respect to varying network size. Figure 4 compares simulation results with the theory for network sizes of 1 to 50 nodes under five different jamming rates. Similarly, we look at the performance comparison of reactive and omniscient jamming in Figures 5 and 6 for varying network sizes and different jamming rates. All of these graphs show nice match between simulation graphs and analytical (theory) graphs.
3. Finally, we compare the effectiveness of different jamming models. Figures 7 and 8 show the performance comparison of the four jammers for two extreme network sizes, 1 session and 50 session network respectively, exchanging 500 byte packets. The group of curves which has a higher throughput under no jamming corresponds to the single session case, and the other group corresponds to the 50 sessions case. It is easy to see that

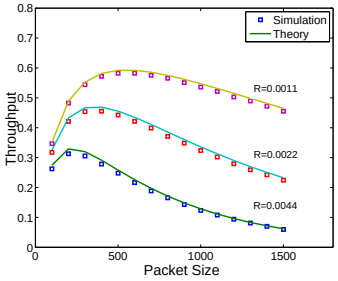


Fig. 3 Throughput of one IEEE 802.11 session under memoryless jamming with different jamming rates.

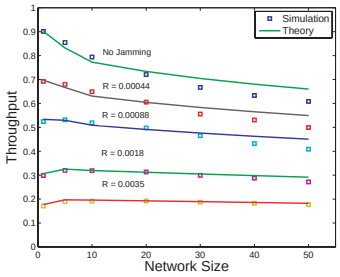


Fig. 4 Throughput of multiple IEEE802.11 sessions under memoryless jamming with different jamming rates.

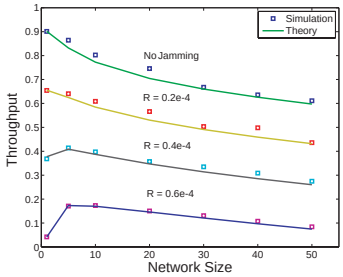


Fig. 5 Throughput of multiple IEEE802.11 sessions under reactive jamming with different jamming rates.

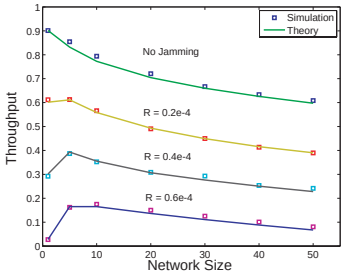


Fig. 6 Throughput of multiple sessions under omniscient jamming with different rates.

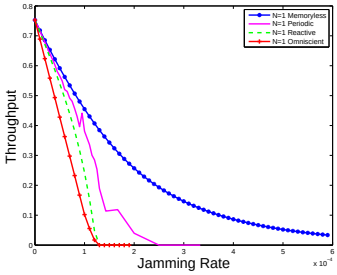


Fig. 7 Comparison of the four jammers. Packet size 500 bytes, 1 802.11 session.

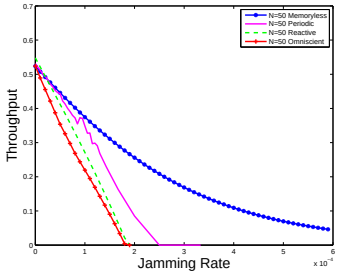


Fig. 8 Comparison of the four jammers. Packet size is 500 bytes, 50 sessions.

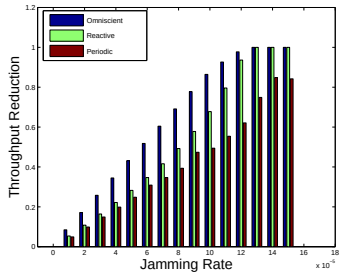


Fig. 9 Jammer efficiency comparison of omniscient, reactive, and periodic jammers. The network size is 1 and the packet size is 500 bytes.

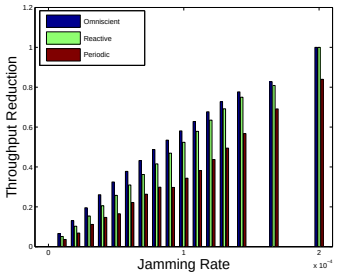


Fig. 10 Jammer efficiency comparison of omniscient, reactive, and periodic jammers. The network size is 50 and packet size 500 bytes.

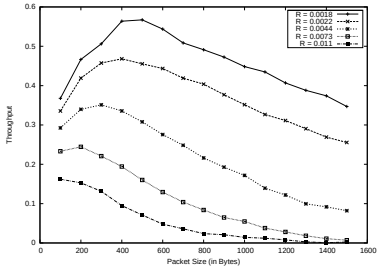


Fig. 11 Experimental throughput for different packet sizes under memoryless jammer with various mean jamming rates.

for a given jamming rate, IEEE802.11 achieves the least throughput under omniscient jamming, followed by the reactive jamming, then periodic jamming with memoryless jamming being least effective. As a general trend, the gap between these jammer performance decreases with an increasing network size. Nevertheless, we observe a difference among them, if we analyze the data carefully. Figures 9 and 10 shows the plot for reduction in the network throughput as a function of jamming rates for periodic, reactive, and omniscient jammers. For a large fraction of the jamming rates, the omniscient jammer reduces the throughput by 20-30% more than a reactive jammer and 20-50% more than a periodic jammer.

5 Experimental Evaluation

In this section, we first discuss the details of our novel testbed designed to implement and evaluate the jamming attacks described in Section 2. We provide the hardware and software components, their specification, testbed setup, and the details of the channel-aware jammer implementation. Then, we present the experimentation methodology and performance metrics along with the performance evaluation of the attacks carried out against IEEE802.11 communication using real world experiments.

5.1 Implementation

5.1.1 Testbed Topology

Our testbed consists of two communication nodes: a sender and a receiver, and the jammer. The sender constantly sends UDP traffic to the receiver to saturate the network. The jammer, if channel-aware, senses the channel for packets and simultaneously decides to jam or not to jam the packet based on the destination address and the jamming probability associated with the jammer. If the jammer is channel-oblivious then it simply jams the channel without sensing using a probability distribution associated with it. Note that for the former scenario of jamming, the jammer must jam the packet before the transmission is over. In fact, we assume that once a jammer transmission overlaps the sender message, the message is completely destroyed. This allows our analysis to focus on the performance of IEEE802.11 MAC layer in the presence of jamming.

Figure 1 depicts such kind of a jammer under our model.

5.1.2 Basic Hardware and Software Components

The hardware components of our testbed include two PCs: (A) a sender node, (B) a receiver node, (C) jammer host[2], (D) the jammer radio along with the RF-cables and (E) splitters/combiners. We chose to use the RF-cabled setup for our experiments because of the following two reasons:

1. To isolate our testbed from the laboratory network.
2. To achieve reproducible results.

Both of these points would be hard to achieve in an open medium. Note that operating the nodes with antennas in an open medium will only make the jamming more effective because of additional collisions/losses due to the propagation environment and external traffic. In this work, our focus is to evaluate the performance of IEEE802.11 in the presence of jamming. Therefore, the use of RF-cables setup in our experimentation is validated, as it only isolates the experimentation tested and does not take away from the performance of the implemented jamming attacks. Furthermore, this type of setup is typical for evaluating wireless channel communication systems for reproducible results using channel emulator [4].

The software components of our testbed include software defined radio (SDR) for signal processing, a traffic generator, a sniffer tool, and the open source wireless card driver that allows for easy reconfiguration of MAC and PHY layer parameters.

Testbed Hardware Specification: We run our experiments on two sets of testbed, one equipped with a USRP board as the jammer radio, and another with a USRP2 board [8]. Figure 12(a) shows the USRP setup, and Figure 12(b) depicts the USRP2 setup. Using USRP or USRP2 only makes a difference when we are implementing channel-aware jammers. USRP is limited by the bandwidth of USB (32 MegaBytes per Second) and response time (reaction time in Figure 1(b)), which prevents the jammer from reacting to the sensing of the messages in the channel within 2 milliseconds. USRP2, on the other hand, uses Gigabit Ethernet to talk to the host and thus is not limited by USB transfer rate. As a result, we observe that the jammer's response time using USRP2 is only a few hundred microseconds ($< 500\mu s$).

Figure 12(a) employs two transceiver daughter boards connected to a USRP motherboard as its sensing and jamming counterparts respectively, and Figure 12(b) employs two individual USRP2s controlled by the same host for sensing and jamming[3]. We picked D-Link WDA-1320 PCI express wireless cards for our sender and receiver wireless radios. They run on Atheros AR5212 chipsets that works with the open source Madwifi driver [3].

Component	Version/Model
Host CPUs	Intel Core2 6300
Jammer Radio	USRP and USRP2
Jammer Radio Daughter boards	RFX-2400
Sender and Receiver Wireless Cards	D-Link WDA-1320 PCI express
Splitter/Combiner	HyperLink SC2402
RF-Cables	L-com RG174 RF-Coaxial Cable

Table 1 Experimental Testbed Hardware Specifications.

Testbed Software Specification: We use GNURadio [7] as the Software Defined Radio (SDR) that supports both USRP and USRP2 jammer radios. Iperf is used as the traffic generator and Wireshark as the sniffer/analyzer tool in our testbed. We use Madwifi driver for the wireless cards, which are very flexible in allowing for easy reconfiguation of MAC and PHY layer parameter settings.

Component	Version/Model
Host OS	Ubuntu v9.10
Sender Traffic Generator	Iperf v2.0.4
Receiver Sniffer/Analyzer	Wireshark v1.2.7
Jammer SDR	GNURadio v3.3.0
Sender and Receiver Wireless Driver	Madwifi v0.9.4

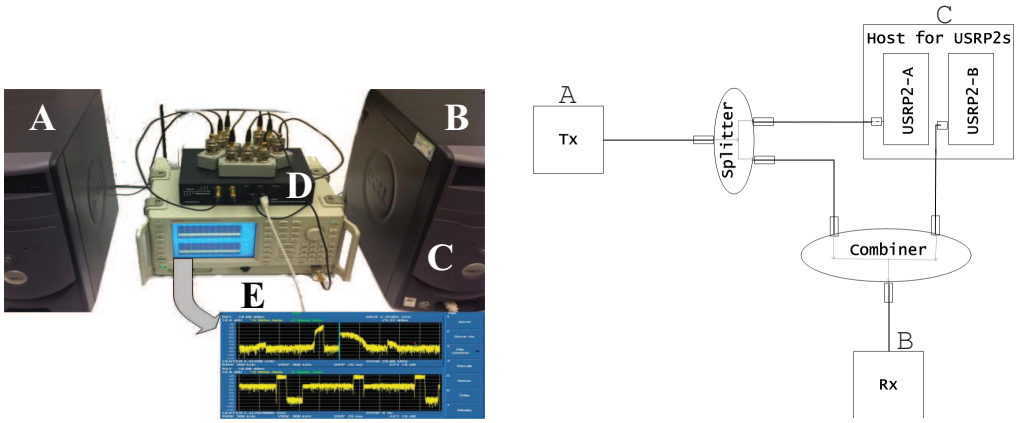
Table 2 Experimental Testbed Software Specifications.

5.1.3 Types of Jammers

For our experimental evaluation, we consider the following four kinds of jammers:

[2] In our testbed, USRP host is one of the communicating nodes. This is not necessary, just for the convenience purposes.

[3] One USRP2 only supports one daughter board.



(a) USRP1-based Testbed (b) USRP2-based Testbed

Fig. 12 Experimentation Testbed: (A) Sender, (B) Receiver, (C) Host for USRP(2)s, (D) USRP(2)s + Splitters + RF-cables, (E) Analyzer.

– **Continuous Jammer:** This jammer produces a continuous signal at a specified power level. We use this kind of jammer to introduce channel noise into our testbed.
– **Periodic Jammer:** This jammer produces a periodic pulse of fixed size enough to destroy a packet if hit. The idle interval is the input to this kind of jammer and is based on the jammer budget as well as the desired network throughput.
– **Memoryless Jammer:** This jammer is similar to the periodic jammer, except the length of the period is decided using a memoryless distribution, the mean of which is the input parameter.
– **Reactive Jammer:** This jammer is channel aware and jams reactively using the information it decodes from the IEEE802.11 PLCP header. This jammer can be memoryless or stateful. In the following, we discuss the implementation of reactive jammer in more detail.

We do not evaluate omniscient jammer's performance experimentally in our testbed. This is because it is relatively hard to implement such a jammer in a real world scenario.

5.1.4 Implementation of the Reactive Jammer

The reactive jammer has two counterparts as shown in Figure 1. The main goal of this jammer is to be able to sniff all the packets in the medium (carried out by C_1 counterpart), and jam the packets destined for the receiver node of interest based on some probability distribution (carried out by the C_2 counterpart). Ideally, a network has multiple sender/receiver links and therefore C_2 has to be able to identify the packets destined for the node of interest by looking into the destination MAC address field. This often requires a fast response/reaction time (time-gap between $C1$ and $C2$ in Figure 1). However, our testbed consistings of USRP software defined radio board has the response/reaction time in the order of milliseconds. Hence, we focus on a single sender/receiver link for our experimental evaluation in this paper and leave the multiple sender/receiver link scenarios for future work, which would require a faster and better radio board.

Therefore, in our current testbed, the sniffer only has to sniff the packets in the channel to figure out the data rate being used for packet transmissions, which requires decoding only the PLCP IEEE802.11 header sent at the robust rate of 1.0Mbps (we disable short preambles), and make jamming decisions to focus on a fixed data rate link of interest. The same hardware limitation of our testbed keeps the jammer from jamming high data rate packets. However, this issue can be resolved without requiring a faster radio board. If we can reduce the bandwidth of IEEE802.11 communication from 20MHz to 5MHz, then it allows jammer to jam higher data rate packets because the bandwidth reduction by a factor of four implies the transmission time of the packet being four time longer than the normal.

In our setup, We use open source Madwifi for our experimentation node's wireless driver which conveniently allows for the narrow band modification.

5.2 Evaluation

In this section, we present the performance of different types of jamming against IEEE802.11 communication. We will first describe the experimentation methodology and the metrics used to evaluate the performance. Then, we will present our experimentation results.

Experimentation Setup: We run our experiments in a RF-cabled setup as described above and depicted in Figure 12. This allowed us to isolate our testbed from the surrounding interference, hence, we were able to achieve results that show very little variance. An experiment run with a fixed set of parameters is defined by the sender continuously sending Constant Bit Rate (CBR) traffic for 50 second period. We rerun the same experiment 10 times each to eliminate the

margin of error, which is already very small for us. We consider a single link scenario with a fixed 1Mbps data communication. We leave the higher data rate experiments for future work.

We would like to note that studying the effect of data rate on an IEEE802.11 network throughput in the presence of jamming would be an interesting topic. However, given that the data rate depends on various factors including coding, modulation, investigating its effect would be a complex problem in itself. Therefore, in this paper, we only focus on understanding the behavior of IEEE802.11 MAC layer. In [22], we have done some preliminary investigation into the topic. We plan to complete the work in the near future.

Parameters: The set of parameters used for experimental evaluation is provided below in Table 5.2.

Parameter	Setting
Packet Size	100-1500 bytes
CBR Rate	1Mbps
Jamming Pulse Width	$22\mu s$
Jamming Rate	$0.0018 - 0.011$
Frequency	2.462 GHz (Channel 11)
Traffic Type	UDP
Traffic Bandwidth	1Mb
Noise Power	-20 dBm

Table 3 Experimentation Parameter Setting.

Performance Metrics: The performance of IEEE802.11 against jamming is measured in terms of the normalized throughput, and the performance of different types of jammers is measured in terms of the throughput reduction attained under a given jamming rate. We obtain various jamming rates for evaluation by varying the idle time interval between two consecutive jammer pulses of fixed width. Therefore, the jamming cost of the jammers can be measured in terms of energy cost or simply the number of jamming pulses sent over a time period.

Note that we assume the ideal jamming conditions for our analysis, i.e., a jamming signal destroys an IEEE802.11 packet completely when their transmissions overlap. We empirically find 22μs to be the appropriate width of the jamming pulse that destroys a 1500 Byte packet sent at $1Mbps$ when hit in our testbed. This size is by no means the optimal value. Since, the main objective of our work is to analyze MAC layer performance of an IEEE802.11 network, we do not engage in optimizing the jamming pulse width in this work. [14] investigates optimal jamming parameters in terms of power efficiency and number of bits to jam.

Evaluation Results:

1. *Memoryless Jammer*: Figure 11 shows the performance of a memoryless jammer against an IEEE802.11 session with different packet sizes under various jamming rates.

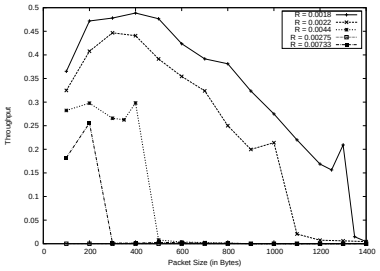


Fig. 13 Experimental throughput for different packet sizes under periodic jammer with various mean jamming rates.

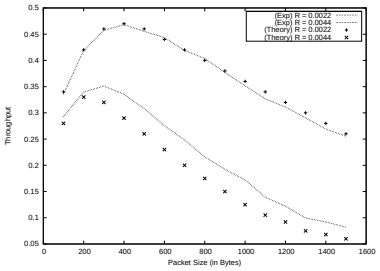


Fig. 14 Experimental and theoretical throughput for different packet sizes under memoryless jammer.

Figure 14 shows that the experimental results are close to the theoretical values and thus validates our analysis.

2. *Periodic Jammer*: Figure 13 shows the performance of a periodic jammer against an IEEE802.11 session with different packet sizes. As we can see, for each jamming rate, there exists a data packet size, x that breaks the trend of the line curve and throughput jumps up before coming back down. This is because when the length of the interval for the periodic jammer becomes close to that of the length of the transmission time (along with the overhead) for the packet with a specific size, x, a jamming pulse misses a packet with high probability. Once it misses, given its the periodic nature, the periodic pulses may miss rest of the packets from that point on with a high probability as well. Therefore, we see the throughput jump. Figure 15 shows that the experimental results are close to the simulation results for periodic jammer when run under the same setup.
3. *Reactive*: Figure 16 shows the performance of reactive jammer with different jamming rates against an IEEE-802.11 session. We observe that there is not much difference in terms of the different packet sizes network when evaluating the reactive jammer performance. This is mainly because at a fixed rate, the larger packets are more vulnerable to reactive jamming than smaller packets. However, the good-put is much higher with larger packets being sent than the smaller ones (due to the overhead) with no jamming present. Thus, under reactive

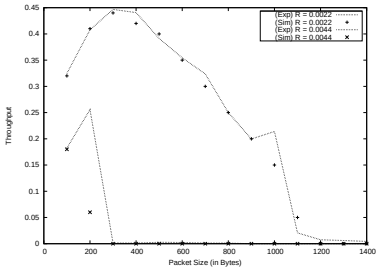


Fig. 15 Experimental and simulation throughput for different packet sizes under periodic jammer.

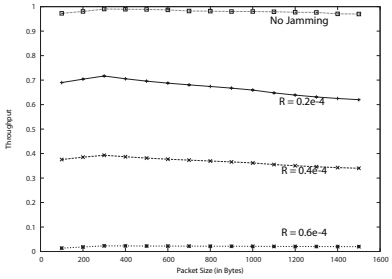


Fig. 16 Experimental throughput for different packet sizes under reactive jammer.

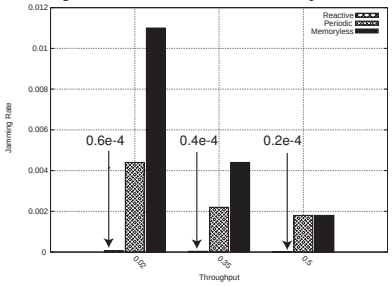


Fig. 17 Jamming cost comparison for different types of jammers.

jamming, the throughput loss almost over the range of varying packet sizes.

4. Jamming cost comparison: Figure 17 shows that to achieve the same throughput reduction, reactive jammer can spend orders of magnitude less energy (less number of jamming pulses) compared to periodic and memoryless. This validates our analysis and simulation results.

6 Discussion and Conclusion

The IEEE802.11 MAC protocol is widely used with support for many physical layers. Given the recent availability of many SDR and sensor networking platforms that make smart jamming relatively easy to build, it is important to understand the limits of IEEE802.11 in the presence of jammers. We have analyzed the saturation throughput performance of IEEE802.11 MAC against several jammers and studied the impact of the jamming rate, packet size, and network size, using mathematical analysis, simulations, as well as a prototype implementation. We note that while we focus our attention on saturation throughput, our results on reactive and omniscient jammers qualitatively extend to unsaturated scenarios; indeed, the effectiveness of these jammers only increases if communication occurs in infrequent bursts.

The four jammers we study are about four orders of magnitude more efficient than a continuous jammer. Among these, the memoryless jammer is the least efficient when compared to the other three jammers. A periodic jammer is easy to implement and is fairly damaging when the network is saturated. It is significantly less effective than the reactive and omniscient jammers for small packet sizes, low number of active sessions, or unsaturated networks. Reactive jammers can dramatically reduce the throughput of IEEE802.11 with only a limited energy cost on the adversary side. Finally, an optimal omniscient jammer is 20-30% more effective than a reactive jammer in reducing throughput; it is especially efficient against networks with a small number of active sessions (as would be typical in practice). Our theoretical analysis has identified (though not completely resolved) the key characteristics of an optimal jammer. Our numerical calculations and simulation suggest a natural conjecture on the structure of the jammer, which we confirmed in special cases.

It would be interesting to completely characterize an optimal jammer for various 802.11 protocol parameters. This would help greatly in the design of anti-jamming techniques. We plan to implement variants of smart jammers using the GNU Radio and USRP family testbed. The new USRP100 platform with embedded processing capabilities will allow a jammer to sense the channel, keep track of retransmissions, and react quickly to transmissions. Partially controllable sensor motes also has the potential to become a low cost small form threat to the IEEE802.11 communication since they are capable of sensing and transmitting in the WiFi band [9]. And, also USRP2 would allow for jamming of higher data rate packets and evaluation of multiple sender/receiver link scenarios. Finally, we would like to investigate if we can learn the state of communicating nodes from an ongoing communication using improved techniques and better hardware/software platform.

References

1. Acharya, M., Sharma, T., Thuente, D., Sizemore, D.: Intelligent jamming in 802.11b wireless networks. In: OPNETWORK (2004)
2. Bellardo, J., Savage, S.: 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In: USENIX (2003)
3. http://madwifi.org/: Multiband atheros driver for wifi
4. http://www.home.agilent.com/agilent/product.jspx?pn=11759C: Agilent technologies rf channel simulator
5. Bianchi, G.: Performance analysis of the ieee802.11 distributed coordination function. IEEE Journal on Selected Areas in Communications **18**(3) (2000)
6. Carvalho, M.M., Garcia-Luna-Aceves, J.J.: Delay analysis of ieee 802.11 in single-hop networks. In: ICNP (2003)

7. http://gnu.org/redmine/wiki/gnuradio: Gnu software defined radio
8. http://www.ettus.com: Universal software radio peripheral
9. http://www.sentilla.com: Moteiv tmote sky
10. Hu, Y.C., Perrig, A., Johnson, D.: Ariadne: A secure on-demand routing protocol for ad hoc networks. In: MOBICOM (2002)
11. IEEE: Medium access control (mac) and physical specifications. IEEE P802.11/D10 (1999)
12. Law, Y.W., van Hoesel, L., Doumen, J., Hartel, P., Havinga, P.: Energy-efficient link-layer jamming attacks against wireless sensor network mac protocols. In: SASN '05 (2005)
13. Li, M., Koutsopoulos, I., Poovendran, R.: Optimal jamming attacks and network defense policies in wireless sensor networks. In: INFOCOM (2007)
14. Lin, G., Noubir, G.: Low-power dos attack in data wireless lans and countermeasures. MobiHoc (2003)
15. Lin, G., Noubir, G.: On link layer denial of service in data wireless lans. Wiley Journal on Wireless Communications and Mobile Computing (2004)
16. Liu, X., Noubir, G., Sundaram, R., Tan, S.: SPREAD: Foiling smart jammers using multi-layer agility. In: INFOCOM Minisymposium (2007)
17. Michael Hall Aki Silvennoinen, S.G.H.: Effect of pulse jamming on IEEE 802.11 wireless LAN performance. In: MILCOM (2005)
18. Monks, J., Bharghavan, V., Hwu, W.: A power controlled multiple access protocol for wireless packet networks. In: INFOCOM (2001)
19. Navda, V., Bohra, A., Ganguly, S., Rubenstein, D.: Using channel hopping to increase 802.11 resilience to jamming attacks. In: INFOCOM Minisymposium (2007)
20. Negi, R., Perrig, A.: Jamming analysis of MAC protocols. Tech. rep., Carnegie Mellon University (2003)
21. http://www.scalable networks.com/: Scalable network technologies
22. Noubir, G., Rajaraman, R., Sheng, B., Thapa, B.: Robustness of IEEE802.11 rate adaptation algorithms against smart jamming. ACM WiSec (2011)
23. Schleher, D.C.: Electronic Warfare in the Information Age. Artech House Inc. (1999)
24. Simon, M.K., Omura, J.K., Scholtz, R.A., Levitt, B.K.: Spread Spectrum Communications Handbook. McGraw-Hill (2001)
25. Thuente, D., Acharya, M.: Intelligent jamming in wireless networks with applications to 802.11b and other networks. In: MILCOM (2006)
26. Ware, C., Wysocki, T., , Chicharo, J.: On the hidden terminal jamming problem in IEEE 802.11 mobile ad hoc networks. In: ICC (2001)
27. Wood, A.D., Stankovic, J.A.: Denial of service in sensor networks. IEEE Computer **35**(10) (2002)
28. Wu, H., Cheng, S., Peng, Y., Long, K., Ma, J.: Ieee 802.11 distributed coordination function: enhancement and analysis. Journal of Computer Science and Technology **18**(5) (2003)
29. Xu, W., Trappe, W., Zhang, Y., Wood, T.: The feasibility of launching and detecting jamming attacks in wireless networks. In: MOBIHOC (2005)
30. Zapata, M., Asokan, N.: Secure ad hoc on-demand distance vector routing. Mobile Comp. and Comm. Review (2002)