# Mitigation of Cascading Denial of Service Attacks on Wi-Fi Networks

Liangxiao Xin
Division of Systems Engineering
Boston University
Boston, MA 02215
Email: xlx@bu.edu

David Starobinski
Division of Systems Engineering
Boston University
Boston, MA 02215
Email: staro@bu.edu

***Abstract*—Recent work demonstrates that IEEE 802.11 networks are vulnerable to cascading DoS attacks, whereby a single node can suddenly render an entire network unstable. In this work, we propose, analyze, and simulate a method to prevent such attacks from occurring. Our key idea is to optimize the duration of packet transmissions. To achieve this goal, we show that it is essential to properly model the impact of MAC overhead, and in particular MAC timing parameters. We propose a new theoretical model where we relate the utilization of neighboring pairs of nodes using a sequence of iterative equations and use fixed point techniques to study the limiting behavior of the sequence. Through this analysis, we show how to optimally set the packet duration so that, on one hand, cascading DoS attacks are avoided and, on the other hand, throughput is maximized. We validate our analytical results using extensive ns-3 simulations. A key insight obtained from our analysis and simulations is that IEEE 802.11 networks with relatively large MAC overhead are less susceptible to cascading DoS attacks than networks with smaller MAC overhead.**

## I. Introduction

The IEEE 802.11 (Wi-Fi) family of standards specify communication protocols that allow users to communicate wirelessly over unlicensed bands (e.g., 2.4 GHz and 5 GHz). Wi-Fi enables ubiquitous access to the Internet and has become the most popular local access network technology. Cisco reports that $42\%$ Internet traffic was transmitted through Wi-Fi in 2015 and that this ratio is expected to increase to $49\%$ by 2020 [1]. Indeed, Wi-Fi is the *de-facto* backbone communication technology for Internet-of-Things (IoT) devices, such as Apple HomePod [2], Amazon Echo [3], and Google Home [4].

Due to the widespread deployment of Wi-Fi networks, ensuring their security is critical. Specifically, the violation of network availability, also known as *Denial-of-Service (DoS)* attack, is a major challenge [5]. Such attacks exploit vulnerabilities at different layers of the protocol stack to degrade network services.

Recent work [6] demonstrates a new and particularly pernicious type of DoS attacks on Wi-Fi networks, called *cascading DoS attack*. This attack exploits an *interference coupling* phenomenon between neighboring cells of IEEE 802.11 networks, which is induced by hidden nodes. Using interference coupling, an attacker can locally raise the amount of traffic that it generates and affect its neighboring cells, which in turn affect their own neighboring cells and so on. As a result, the transmitting queue of a distant node can suddenly be brought into instability and get saturated. The attack is feasible in both infrastructure and ad-hoc networks, under certain configurations. Moreover, since the attack can be launched remotely and is protocol compliant, it makes it difficult to locate and identify the attacker. Given the serious consequences of cascading DoS attacks, it is important to find methods to mitigate them.

In this paper, we focus on the mitigation of cascading DoS attacks in Wi-Fi networks. Our key idea is to optimize the durations of packet transmissions (or, equivalently, the packet length divided by the bit rate) in order to ensure that interference coupling does not propagate and amplify. To achieve this goal, we show that it is essential to properly model the impact of MAC overhead, and in particular MAC timing parameters. We propose a new theoretical model where we relate the utilization of nodes in neighboring cells using iterative equations. We then perform a fixed point analysis to characterize the limiting behavior of the sequence of node utilizations and the feasibility of launching a cascading DoS attack against a Wi-Fi network.

Our main contributions are as follows. We first show how to set the packet duration in order to avoid a cascading DoS attack, namely to prevent the initial value of the sequence of node utilizations (which can be set by the attacker) to affect the limit of the sequence. Second, we show that it is possible to simultaneously optimize the packet duration in order to achieve maximum throughput. Third, we validate the analytical results using ns-3 simulations, including for an office building model. A key insight obtained from our analysis and simulation is that IEEE 802.11 networks with relatively large MAC overhead (e.g., IEEE 802.11b) are less susceptible to cascading DoS attacks than networks with smaller overhead (e.g., IEEE 802.11g and IEEE 802.11n). We also show that our method achieves higher throughput performance than the RTS/CTS method, especially at high bit rates.

The rest of this paper is organized as follows. In Section II, we discuss related work and necessary background on the IEEE 802.11 standard. In Section III, we explain how cascading DoS attacks operate and the impact of the packet length on the feasibility of launching such attacks. In Section IV, we introduce our analytical model, derive a sufficient condition

for preventing cascading DoS attacks, and show how to optimally set packet durations in order to maximize throughput performance. We present our simulation results in Section V, and conclude in Section VI. Due to space constraints, some proofs are abbreviated or omitted.

## II. Related Work and Background

### A. Related work

The goal of a DoS attack is to impair network services. Traditional jamming attacks [7] use high transmission power to create interference and congest a network. More recently, *smart jamming* techniques have been developed and demonstrated to achieve high efficiency and anti-detection capabilities [8]. However, those attacks require physical proximity and focus on a single cell. In contrast, a cascading DoS attack can propagate through multiple cells and be launched from a remote location.

The work in [6] theoretically and empirically demonstrates a cascading DoS attack in Wi-Fi networks. The analysis in [6] shows that a cascading DoS attack is feasible when the retry limit parameter is greater or equal to 7. In our work, we investigate theoretically and by simulations a method to prevent cascading DoS attack, which is based on optimizing the packet duration. Our analysis captures the effect of MAC overhead (which is ignored in [6]). We show that our solution is effective even when the retry limit is set to 7 (which is the default value in Wi-Fi).

The effect of MAC timing parameters on the performance of IEEE 802.11 networks has been extensively studied in the literature [9]–[16]. In particular, an analysis carried out in [16] shows that in the absence of contention between nodes, MAC overhead significantly affects throughput, especially at high bit rates. In contrast to those papers, the focus of our paper is to assess the impact of the MAC overhead on the feasibility of launching a cascading DoS attack. Interestingly, we show that a larger MAC overhead can help prevent such attacks (by mitigating the impact of hidden nodes).

Interference coupling caused by hidden nodes is studied by [17]–[19], though none of these works consider security ramifications. The work in [17] shows that coupling causes nodes to transmit at low bit rates, thus aggravating packet losses. The work in [18] conducts a queuing-theoretic analysis of a chain of neighboring cells with hidden nodes. The analysis reveals that the impact of hidden nodes propagates through the network, causing some nodes to saturate at load as low as 15% of the capacity.

The work in [19] perform measurements of a multi-cell IEEE 802.11 network in an indoor testbed. The experiments clearly shows the existence of hidden nodes and the effects of interference coupling in a real world setting. The experimental results also show that hidden nodes cause fairness issues. These fairness issues as well as throughput performance of the network get even worse when RTS/CTS is enabled. Other drawbacks of the RTS/CTS procedure are discussed in [20], [21].

### B. IEEE 802.11 Standard

We next provide details about the IEEE 802.11 standard and in particular the MAC timing parameters of different variants of the standard (i.e., b/g/n). As shown in the sequel, these MAC parameters play an important role in determining the feasibility of launching a cascading attack against IEEE 802.11 networks.

The IEEE 802.11 standard uses carrier sense with collision avoidance to control access of nodes to the shared medium. When a node senses the channel to be idle, it waits for a distributed interframe space (DIFS) followed by a random backoff delay before transmitting a packet. The backoff delay consists of a random number of backoff slots. The range of possible backoff slots depends on the contention window. Specifically, at the $r \geq 1$ retransmission attempt, the contention window is given by

$$CW_r = \begin{cases} 2^{r-1}(CW_1 + 1) - 1 & CW_r < CW_{\max}, \\ CW_{\max} & \text{otherwise}, \end{cases} \quad (1)$$

where $CW_1$ represents the initial contention window and $CW_{\max}$ represents the maximum possible size of a contention window. The parameter $r$ is referred to as the *retry count*. Note that $r = 1$ corresponds to the first transmission attempt.

The number of backoff slots is an element of the set $\{0, 1, \ldots, CW_r\}$ chosen uniformly at random. We denote the duration of a backoff slot by $T_{\text{slot}}$. The average backoff delay at the $r$th retransmission attempt is

$$\overline{T}_{\text{backoff},r} = \frac{1}{2} CW_r \cdot T_{\text{slot}}. \quad (2)$$

After sending a packet, a node waits for a short interframe space (SIFS) period before expecting to receive an ACK. If the ACK is received (i.e., the transmission is successful), then the average duration of the MAC overhead at the $r$th retransmission attempt is

$$d_r^{(s)} = T_{\text{DIFS}} + \overline{T}_{\text{backoff},r} + T_{\text{SIFS}} + T_{\text{ACK}}, \quad (3)$$

where $T_{\text{DIFS}}$ and $T_{\text{SIFS}}$ represent respectively the durations of the DIFS and SIFS intervals and $T_{\text{ACK}}$ represents the duration of an ACK transmission.

If a node does not receive an ACK within an *ACK timeout* period (e.g., due to a collision caused by a hidden node), then it increments $r$ and repeats the procedure. Thus, if a transmission fails, the average duration of the MAC overhead at the $r$th retransmission attempt is

$$d_r^{(f)} = T_{\text{DIFS}} + \overline{T}_{\text{backoff},r} + T_{\text{ACK\_timeout}}, \quad (4)$$

where $T_{\text{ACK\_timeout}}$ is the duration of the ACK timeout interval. This process continues as long as the number of retransmissions $r$ does not exceed the (short) retry limit $R$. Once this limit is exceeded, the packet is dropped, $r$ is reset to 1, and the transmission of a new packet can start. In all our analysis and simulations, we use the default value of the retry limit, namely $R = 7$ [22].

The IEEE 802.11 standard has several variants, which differ in their physical and MAC layer specifications [23]. These variants support transmissions at different bit rates going up

TABLE I: IEEE 802.11 parameters [25]

| | 802.11b | 802.11g/n |
|---|---|---|
| $CW_1$ | 31 | 15 |
| $CW_{\max}$ | 1023 | 1023 |
| $T_{\text{DIFS}}$ ($\mu$s) | 50 | 28 |
| $T_{\text{SIFS}}$ ($\mu$s) | 10 | 10 |
| $T_{\text{slot}}$ ($\mu$s) | 20 | 9 or 20 |

to 11 Mb/s for IEEE 802.11b, 54 Mb/s for IEEE 802.11g, and 600 Mb/s (theoretically) for IEEE 802.11n. In practice, IEEE 802.11n networks often operate with bit rates going up to 54 Mb/s [23].

Table I shows settings of the timing parameters of IEEE 802.1b and IEEE 802.11g/n that are relevant to this paper. Note that IEEE 802.11g/n networks can use either a long slot time (i.e., $T_{\text{slot}} = 20$ $\mu$s) or a short slot time (i.e., $T_{\text{slot}} = 9$ $\mu$s) [24]. The long slot time is typically used in a mixed environment composed of both 802.11b and 802.11g/n nodes.

## III. Cascading DoS Attacks

### A. Attack scenario

We next explain how a cascading DoS attack can unfold. We consider a network configuration consisting of a chain of $N$ pairs of nodes [6]. Figure 1 depicts the configuration. The $i$th pair is denoted $(A_i, B_i)$, where $i \geq 1$. Each node $A_i$ transmits packets to node $B_i$ (one-hop communication). Furthermore, each node $A_i$ is a *hidden node* with respect to node $A_{i+1}$, which means that node $A_i$ cannot sense a transmission by node $A_{i+1}$. If a transmission by node $A_i$ overlaps with a transmission by node $A_{i+1}$, a packet collision occurs at node $B_{i+1}$. This collision forces node $A_{i+1}$ to retransmit its packet using the procedure described in Section II-B.

In this configuration, suppose node $A_1$ (the attacker) starts increasing the rate at which it generates packets and transmits them over the channel (in compliance with the IEEE 802.11 standard). These transmissions will cause collisions at node $B_2$, which forces node $A_2$ to increase the rate at which it attempts to transmit packets over the channel (due to retransmissions). The increased rate of transmission attempts by $A_2$ will in turn impact pair $(A_3, B_3)$ and so forth. Under certain conditions, this effect may amplify along the chain and cause a large fraction of transmission attempts to fail and result in unstable queues (i.e., the rate at which nodes can successfully transmit packets over the channel is lower than the rate at which packets are generated).

### B. Example

To help motivate the rest of this paper, we next present an example to illustrate the occurrence of a cascading DoS attack in a practical scenario, as well as a way to prevent it. Define $\rho_i$ as the *offered load* at node $i$, that is, the rate at which it generates packets multiplied by the transmission duration of each packet. Further, define the *utilization* of node $A_i$ as the average fraction of time during which node $A_i$ is transmitting,

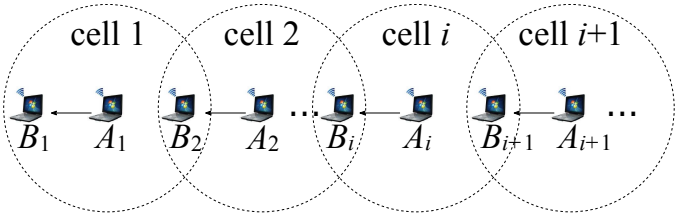



Fig. 1: Network configuration. The dotted circles represent the communication range of nodes $A_i$. Nodes $A_i$ transmit packets to nodes $B_i$ $(i = 1, 2, \ldots)$. Each transmission pair $(A_i, B_i)$ belongs to a different cell. Nodes $A_i$ are hidden nodes with respect to nodes $A_{i+1}$.

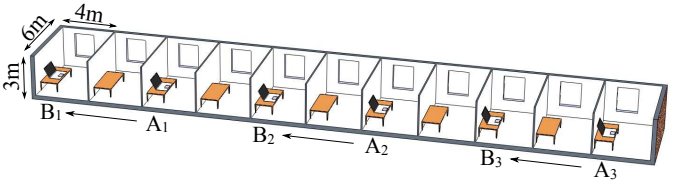



Fig. 2: Example of an attack in an office building. Three transmission pairs $(A_i, B_i)$, where $i \in \{1, 2, 3\}$, are positioned as shown in the figure.

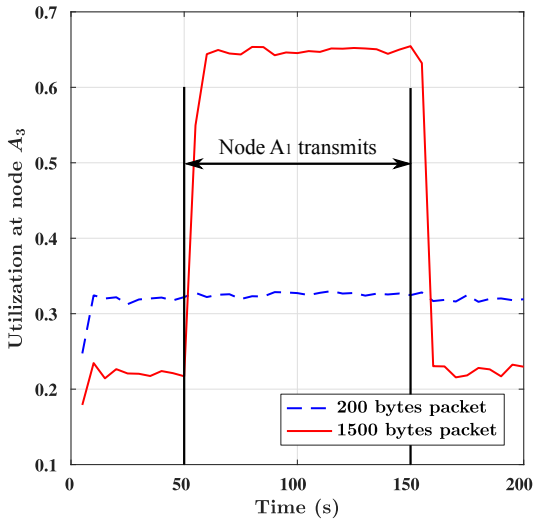
and the *throughput* of node $A_i$ as the average number of bits per second that node $A_i$ successfully transmits to node $B_i$.

As shown in Figure 2, we consider communication within an office building using the ns-3 building model [26]. The external wall of the building is made of concrete with windows. The internal wall loss is 12 dB [27]. All the other parameters are set to default. In the following two examples, we consider an IEEE 802.11g/n network composed of $N = 3$ pairs of nodes and communicating using UDP (examples of realistic applications using UDP include Google Chromecast and Apple TV).

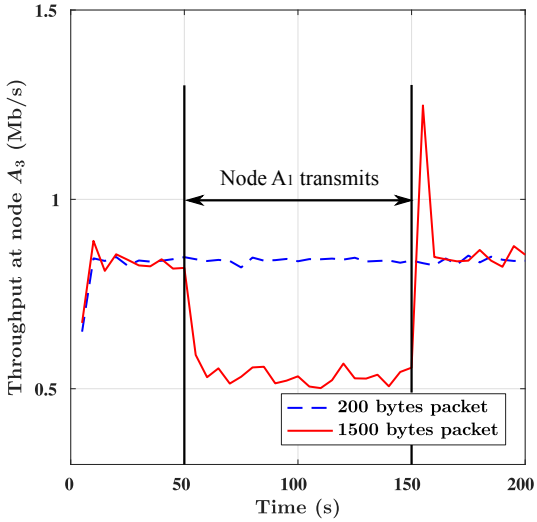
The nodes are located in every other room, as shown in Figure 2. Each transmitting node uses a short slot time (i.e., $T_{\text{slot}} = 9$ $\mu$s) and a bit rate of 6 Mb/s. The offered load at nodes $A_2$ and $A_3$ is set to 0.14 while the attacker $A_1$ varies its load $\rho_1$. We run simulations of this configuration using the ns-3 simulator [26]. The running time of each simulation is 200 seconds and the plotted results are averages computed over three independent runs.

In the first example, we set the packet length to 1500 bytes. Simulation results illustrating the cascading attack are depicted in Figure 3. We observe that as node $A_1$ starts to transmit after 50 s, the utilization of node $A_3$ suddenly jumps from about 0.25 to 0.65 due to packet collisions and retransmissions. As a result, its throughput drops from about 0.75 Mb/s to 0.5 Mb/s. The utilization and throughput of node $A_3$ recovers once node $A_1$ stops transmitting after 150 s.

Now consider the same setting, but with packets of length 200 bytes. The offered load of nodes $A_2$ and $A_3$ is maintained the same as in the previous example (by increasing the packet generation rate). In that case, we observe that increased traffic generation by node $A_1$ has no effect on the utilization and




(a) Utilization.




(b) Throughput.

Fig. 3: Feasibility of cascading DoS attacks in IEEE 802.11g/n networks of an office building. When nodes in the network use 1500 bytes packets, node $A_1$ can launch a cascading DoS attack. When node $A_1$ is transmitting, node $A_3$ suffers from low throughput and high channel utilization. However, this attack is prevented when nodes use 200 bytes packets.

throughput of node $A_3$. This result holds no matter what packet length is used by the attacker.

The work of [6] only considers the impact of the traffic load and the retry limit on the feasibility of a cascading attack. Figure 3 clearly shows that this is insufficient and that other parameters (e.g., the packet length) need to be taken into account. In the next section, we present and analyze a model that incorporates these other parameters.

## IV. Mitigation of Cascading Attacks: Model and Analysis

We propose an analytical model to find out how to mitigate a cascading DoS attack against an IEEE 802.11 network. The proposed model captures key system parameters, including the offered load, the packet duration (i.e., the packet length divided by the bit rate), and MAC parameters. We consider the network configuration shown in Fig. 1, since it is a configuration for which it is known that cascading attacks are feasible [6]. The analysis captures the coupling between the utilizations of neighboring pairs of nodes in the chain through a sequence of iterative equations. We conduct a fixed point analysis to determine the limit of the sequence, as a function of the initial condition (i.e., the utilization of the first node in the chain, which is the attacker). Our goal is to determine when the initial value of the sequence of utilization is guaranteed to have no influence on the limit of the sequence (that is, the utilization of remote nodes) for all possible traffic loads.

### A. Model and assumptions

We now present our model, notation, and assumptions. We denote by $\lambda_1$ the packet generation rate at node $A_1$ (the attacker) and by $\lambda_i = \lambda$ the packet generation rate at all the other nodes $A_i$ ($i \geq 2$). The duration of a packet transmission is $T$ (we assume a fixed bit rate). The offered load at node $A_1$ is $\rho_1 = \lambda_1 T$ and the offered load at all the other nodes is $\rho = \lambda T$. The average number of transmissions for each packet at node $A_i$ (i.e., the average retry count) is denoted $\overline{r}_i$. Note that $\overline{r}_1 = 1$. The probability that a packet transmitted by node $A_i$ collides is denoted $p_i$. Finally, we denote by $\mu_i$ the service capacity of the channel, that is the maximum average rate at which packets (both new and retransmissions) can be transmitted over the channel. In the sequel, we derive expressions for $\overline{r}_i$, $p_i$ and $\mu_i$.

The utilization of node $A_i$ (i.e., the fraction of time during which it transmits) is denoted $u_i$. If $\overline{r}_i\lambda_i < \mu_i$, then the queue of node $A_i$ is stable and by Little's Law [28] its utilization is $\overline{r}_i\lambda_i T$. On the other hand, If $\overline{r}_i\lambda_i > \mu_i$, then the queue of node $A_i$ is unstable and its utilization is $\mu_i T$. We refer to $\mu_i T$ as the *saturated utilization*. Hence, the utilization of node $A_i$ ($i \geq 1$) is

$$u_i = \min\{\overline{r}_i\lambda_i T, \mu_i T\}. \tag{5}$$

In order to render the analysis of this queueing network tractable, we make use of Kleinrock's random look assumption [29], namely:

1) The probability $p_i$ that a packet transmitted by node $A_i$ collides is independent of previous attempts.
2) Packet transmissions and retransmissions at each node $A_i$ form a Poisson process with rate $\min\{\overline{r}_i\lambda_i, \mu_i\}$.

We emphasize that beside these approximations, the rest of the analysis is exact. Note that a key difference between the analysis conducted in our paper and [6] is that we develop a method to characterize the saturated utilization (see Lemma 3). Because the saturation utilization is smaller than 1, the structure

of the iterative sequence (see Eq. (14)) and the analysis of its limits (see Sections IV-C to IV-E) are markedly different from the results derived in [6].

### B. Iterative analysis

In this section, we derive iterative equations for relating the utilizations of neighboring pairs of nodes. The following lemma provides expressions for $p_i$ and $\overline{r}_i$. The proof follows similar lines as the derivations of Equations (6) and (7) in [6].

*Lemma 1:* For $i \geq 2$,

1) $p_i = 1 - \mathrm{e}^{-u_{i-1}}(1 - u_{i-1})$. (6)
2) $\overline{r}_i = \sum_{r=1}^{R} p_i^{r-1}$. (7)

Using the above lemma, one can obtain an expression for the average utilization of a node with a stable queue.

*Lemma 2:* Let $i \geq 2$ and suppose that the queue of node $A_i$ is stable. Then its utilization is

$$\overline{r}_i \lambda T = \rho \sum_{r=1}^{R} \left(1 - \mathrm{e}^{-u_{i-1}}(1 - u_{i-1})\right)^{r-1}. \quad (8)$$

We next provide an expression for the saturated utilization of a node with an unstable queue.

*Lemma 3:* Let $i \geq 2$ and suppose that the queue of node $A_i$ is unstable. Then its saturated utilization is

$$\mu_i T = \frac{\sum_{r=1}^{R} p_i^{r-1} T}{\sum_{r=1}^{R} p_i^{r-1}(d_r^{(s)}(1-p_i) + d_r^{(f)} p_i + T)},$$

where $d_r^{(s)}$, $d_r^{(f)}$ and $p_i$ are given by Equations (3), (4) and (6) respectively.

*Proof:* Define the backoff cycle of a packet as the time it takes for that packet to be successfully transmitted during a back-off procedure or dropped after $R$ failed retransmissions. We note that the lengths of backoff cycles of different packets are independent, due to Assumption 1 and the fact that the contention window is reset at the beginning of each cycle. Hence, the backoff process of consecutive packets forms a regenerative process [30], which implies that the average utilization of node $A_i$ is the ratio of the average time during which node $A_i$ transmits during a backoff cycle to the average length of a backoff cycle.

Now, the fact that node $A_i$ retransmits a packet for the $r$th time implies that all the previous $r-1$ retransmissions failed due to packet collisions caused by a hidden node. Hence, the probability that node $A_i$ transmits a packet at least $r$ times is $p_i^{r-1}$ and the average time that node $A_i$ spends transmitting during a backoff cycle is

$$\sum_{r=1}^{R} p_i^{r-1} T. \quad (9)$$

The average time that node $A_i$ spends on the $r$th retransmission is $d_r^{(s)}(1-p_i) + d_r^{(f)} p_i + T$. Hence, the average length of a backoff cycle is

$$\sum_{r=1}^{R} p_i^{r-1}(d_r^{(s)}(1-p_i) + d_r^{(f)} p_i + T). \quad (10)$$

Taking the ratio of Eq. (9) to Eq. (10) gives the result stated by the lemma. ∎

To simply notation in the rest of the analysis, we define the following functions based on Lemmas 1, 2 and 3:

$$P(u_{i-1}) \triangleq p_i = 1 - \mathrm{e}^{-u_{i-1}}(1 - u_{i-1}); \quad (11)$$

$$U(u_{i-1}) \triangleq \overline{r}_i \lambda T = \rho \sum_{r=1}^{R} \left(1 - \mathrm{e}^{-u_{i-1}}(1 - u_{i-1})\right)^{r-1}; \quad (12)$$

$$S(u_{i-1}) \triangleq \mu_i T = \frac{\sum_{r=1}^{R} (p_i)^{r-1} T}{\sum_{r=1}^{R} ((p_i)^{r-1}(d_r^{(s)}(1-p_i) + d_r^{(f)} p_i + T))}. \quad (13)$$

Substituting (12) and (13) into (5), we obtain the following relationship between the utilizations of nodes $A_i$ and $A_{i-1}$:

$$u_i = \min\left\{U(u_{i-1}), S(u_{i-1})\right\}. \quad (14)$$

### C. Limiting behavior and fixed points

We next characterize the limiting behavior of the sequence of utilizations, using the concept of fixed points. We then formalize the notion of a cascading DoS attack, and obtain a sufficient condition for preventing it.

Consider the possible limits of the utilization sequence $\{u_i\}_{i=1}^{\infty}$. These limits represent *fixed points* of the iteration (14).

*Definition 1 (Fixed point):* We say that $\omega \in [0, 1]$ is a fixed point of (14) if

$$\omega = \min\left\{U(\omega), S(\omega)\right\}. \quad (15)$$

We next define the two possible types of fixed points.

*Definition 2 (Saturated and unsaturated fixed points):* Let

$$\breve{\omega} = U(\breve{\omega}). \quad (16)$$

If $\breve{\omega}$ also satisfies (15), we say that $\breve{\omega}$ is an *unsaturated fixed point*. Likewise, let

$$\hat{\omega} = S(\hat{\omega}). \quad (17)$$

If $\hat{\omega}$ also satisfies (15), then we say that $\hat{\omega}$ is a *saturated fixed point*.

Based on the property of a fixed point (i.e., saturated or unsaturated), we define next whether a network is saturated or not.

*Definition 3 (Network saturation):* A network is said to be *unsaturated* if the limit of the utilization sequence $\{u_i\}_{i=1}^{\infty}$ is an unsaturated fixed point $\breve{\omega}$. Otherwise, if the limit of the utilization sequence $\{u_i\}_{i=1}^{\infty}$ is a saturated fixed point $\hat{\omega}$, then the network is said to be *saturated*.

Using the above notions, we now formally define a cascading DoS attack.

*Definition 4 (Cascading DoS attack):* A cascading DoS attack occurs when changing $u_1$ causes the network to change its state from unsaturated to saturated.

We conclude that an attack is feasible only if the utilization sequence has both unsaturated and saturated fixed points. If

for each possible value of the offered traffic load $\rho$, (15) has only one type of fixed points, then a cascading DoS attack can never be launched on the network (assuming that all the other network parameters remain fixed).

In the following, we show that the value of $\hat{\omega}$ plays a key role in determining the feasibility of launching a cascading DoS attack. Specifically, we show that if $\hat{\omega} \leq (3-\sqrt{5})/2$, then (15) has only one type of fixed points for each traffic load $\rho$ and a cascading DoS attack is unfeasible. In Section IV-F, we further show that if $\hat{\omega} = (3-\sqrt{5})/2$, then the network achieves the highest possible saturation throughput.

### D. Existence of fixed points

We now investigate the existence of the two types of fixed points (unsaturated and saturated) in Equation (15). We first show that if a saturated fixed point exists, then it is unique.

*Lemma 4:* Eq. (17) has a unique solution $\hat{\omega}$.

*Proof:* We show that the function $F(\omega) \triangleq S(\omega) - \omega$ is continuous and strictly decreasing in the interval $[0,1]$ with $F(0) > 0$ and $F(1) < 0$. Therefore, according to the intermediate value theorem [31], there exists a unique solution $F(\hat{\omega}) = 0$ (i.e., $S(\hat{\omega}) = \hat{\omega}$).

According to (11), $P(0) = 0$. Therefore,

$$\begin{aligned} &F(0) = S(0) - 0 \\ =&\frac{\sum_{r=1}^{R}(P(0)^{r-1}T)}{\sum_{r=1}^{R}((P(0))^{r-1}(d_r^{(s)}(1-P(0)) + d_r^{(f)}P(0) + T))} \\ =&\frac{T}{T + d_1^{(s)}} > 0. \end{aligned}$$

Since $S(\omega)$ is always strictly smaller than 1 (due to the MAC timing constants that only appear in the denominator), we have

$$F(1) = S(1) - 1 < 0.$$

It remains to prove that the derivative of $F(\omega)$ is always negative in the interval $[0,1]$. That is,

$$\frac{d(S(\omega)-\omega)}{d\omega} = \frac{dS(\omega)}{dP(\omega)} \cdot \frac{dP(\omega)}{d\omega} - 1 < 0.$$

The derivative of $P(\omega)$ is

$$\frac{dP(\omega)}{d\omega} = e^{-\omega}(1-\omega) + e^{-\omega} = e^{-\omega}(2-\omega) > 0.$$

Using algebra, one can prove that $\frac{dS(\omega)}{dP(\omega)}$ is negative for all $\omega \in [0,1]$, which proves the result. ■

We next determine when a saturated fixed point exists at $\hat{\omega}$, for a given traffic load $\rho$. Based on (15), such a fixed point must satisfy

$$\hat{\omega} \leq U(\hat{\omega}). \tag{18}$$

Let

$$G(\omega) \triangleq \frac{\rho\omega}{U(\omega)} = \frac{\omega}{\sum_{r=1}^{R}\left(1 - \mathrm{e}^{-\omega}(1-\omega)\right)^{r-1}}. \tag{19}$$

The following lemma follows directly from (18) and (19).

*Lemma 5:* A saturated fixed point exists at $\hat{\omega}$ if and only if $\rho \geq G(\hat{\omega})$.

The following lemma establishes when an unsaturated fixed point exists.

*Lemma 6:* An unsaturated fixed point exists if and only if $\rho \leq \max_{\omega\in[0,\hat{\omega}]} G(\omega)$.

### E. Avoidance of cascading DoS attacks

We next establish a sufficient condition to avoid a cascading DoS attack on a network. According to Definition 4, a cascading DoS attack is unfeasible if Equation (15) has only one type of fixed points (i.e., either unsaturated or saturated) for each $\rho$. Hence, we provide the following lemma.

*Lemma 7:* If $G(\hat{\omega}) > G(\omega)$ for all $\omega \in [0,\hat{\omega})$, then Equation (15) has only one type of fixed points for each traffic load $\rho > 0$.

*Proof:* The result follows directly from Lemma 5 and 6. When $\rho > G(\hat{\omega})$, only a saturated fixed point exists, while when $\rho < G(\hat{\omega})$, only one (or more) unsaturated fixed points exist. Note that in the special case $\rho = G(\hat{\omega})$ , there exists a unique fixed point $\hat{\omega}$ that is both saturated and unsaturated since $U(\hat{\omega}) = S(\hat{\omega})$. This boundary case is similar to when the server load equals 1 in a queueing system. Nevertheless, since the fixed point is unique, an attacker cannot impact the limiting fixed point in that case either. ■

Let

$$\alpha \triangleq \frac{3-\sqrt{5}}{2} \approx 0.38. \tag{20}$$

We now state our first main result.

*Theorem 1 (Prevention of cascading attacks):* A cascading DoS attack is unfeasible if $\hat{\omega} \leq \alpha$, where $\hat{\omega}$ is the unique solution of (16) and $\alpha$ is given by (20).

*Proof:* Using algebra, the function $G(\omega)$ can be shown to be strictly increasing in the interval $[0,\alpha]$. The result then follows by Lemma 7. ■

The above theorem implies that an attacker cannot launch a cascading DoS attack, if $\hat{\omega}$ is kept sufficiently low.

### F. Optimizing the saturation throughput

In this section, we optimize the packet duration to achieve the highest throughput performance when the network is saturated. We remind that the throughput of node $A_i$ is defined as the average number of bits per second that it successfully transmits to node $B_i$ (this quantity is also sometimes referred to as goodput in the literature). The *saturation throughput* is the throughput of a node when packets are always waiting in its queue (i.e., when the queue is unstable). The saturation throughput can be found by taking the product of the saturated utilization with the probability that a packet does not get lost. As $i$ get large (i.e., looking at a node far down in the chain), the saturated utilization of node $A_i$ converges to $S(\hat{\omega}) = \hat{\omega}$ and the packet loss probability converges to $P(\hat{\omega})$, where the functions $P(\cdot)$ and $S(\cdot)$ are defined in Eqs. (11) and (13), respectively. The saturation throughput is therefore given by

$$\begin{aligned} X(\hat{\omega}) &\triangleq (1 - P(\hat{\omega})) \cdot \hat{\omega} \\ &= e^{-\hat{\omega}}(1-\hat{\omega}) \cdot \hat{\omega}. \end{aligned} \tag{21}$$

Eq. (21) implies that the saturation throughput $X(\hat{\omega})$ does not always increase with $\hat{\omega}$. The following theorem determines the value of $\hat{\omega}$ that optimizes $X(\hat{\omega})$.

*Theorem 2 (Optimal saturation throughput):* The maximum saturation throughput is achieved at $\hat{\omega} = \alpha$, where $\alpha$ is given by (20).

*Proof:* Let $\hat{\omega} \in [0, 1]$. According to (21), the derivative of $X(\hat{\omega})$ is

$$X'(\hat{\omega}) = e^{-\hat{\omega}}(1 - 3\hat{\omega} + \hat{\omega}^2). \tag{22}$$

There exists a unique solution of the equation $X'(\hat{\omega}) = 0$ at $\hat{\omega} = \alpha$. Since the second order derivative of $X(\hat{\omega})$ is negative at $\hat{\omega} = \alpha$, that is,

$$X''(\alpha) = e^{-\alpha}(-4 + 5\alpha - \alpha^2) < 0,$$

we conclude that $X(\alpha)$ is the maximum of $X(\hat{\omega})$ in the interval $\hat{\omega} \in [0, 1]$. ■

Combined with Theorem 1, we obtain the remarkable result that $\hat{\omega} = \alpha$ both prevents cascading DoS attacks and maximizes the saturation throughput.

By setting $\hat{\omega} = \alpha$, we can calculate the optimal packet duration $T^*$ that maximizes the saturation throughput. Specifically substituting $\hat{\omega} = \alpha$ into (17) and using (13), we get

$$T^* = \frac{\alpha \sum_{r=1}^{R} (P(\alpha))^{r-1} (d_r^{(s)}(1 - P(\alpha)) + d_r^{(f)} P(\alpha))}{(1 - \alpha) \sum_{r=1}^{R} (P(\alpha))^{r-1}}. \tag{23}$$

Note that for any bit rate, the optimal packet length can be found by multiplying the optimal packet duration with the bit rate.

According to (23), the optimal packet duration is affected by the MAC overhead parameters. In particular, the optimal packet duration in IEEE 802.11b networks is longer than in 802.11g/n networks. Using the parameters shown in Table I the optimal packet duration in IEEE 802.11b is $T^* = 1.10$ ms, while in IEEE 802.11g/n with long slot time $T^* = 0.65$ ms and with short slot time $T^* = 0.27$ ms.

## V. Simulation Results

We next present simulation results using ns-3 [26]. We first demonstrate the importance of properly modeling MAC timing parameters in the context of cascading DoS attacks (the impact of the packet length was shown in Section III-B). We then validate the accuracy of our analytical model in predicting the saturated utilization of a network. Finally, we verify Theorems 1 and 2, and compare the performance of our method (based on optimizing the packet duration) to an RTS/CTS-based method. All the simulations shown in this section assume that the retry limit $R$ is set to 7 and nodes communicate using UDP. Each simulation is run for 200 seconds and the plotted results are averages computed over three independent runs.

### A. Impact of MAC timing parameters

We compare the behavior of IEEE 802.11g/n networks using respectively a long slot time (i.e., $T_{\text{slot}} = 20$ $\mu$s) and a short slot time (i.e., $T_{\text{slot}} = 9$ $\mu$s). All the other system parameters are identical. The network contains 20 pairs of nodes (see Fig. 1). Each node $A_i$ transmits 1500 bytes packets at 6 Mb/s bit rate to node $B_i$ $(i = 1, 2, \ldots, 20)$. The offered load of nodes $A_i$ $(i \geq 2)$ is set to $\rho = 0.14$.

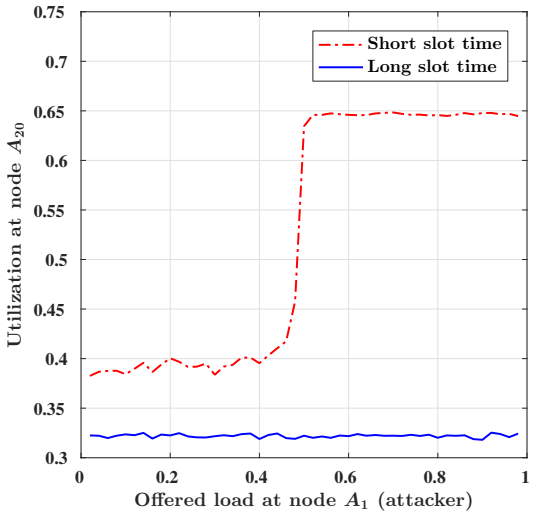


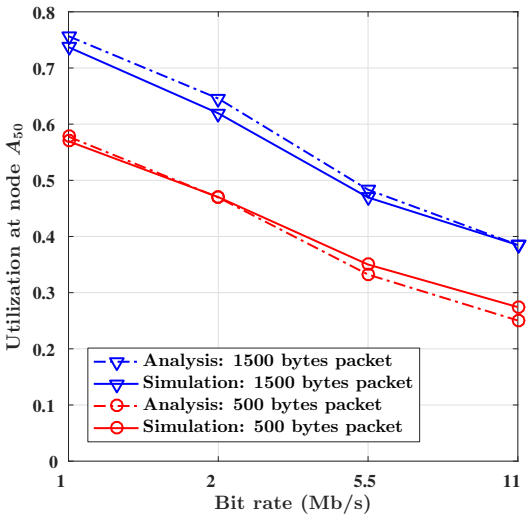

Fig. 4: IEEE 802.11g/n networks under different MAC configurations. With a short slot time $T_{\text{slot}} = 9$ $\mu$s, a cascading DoS attack occurs. However, the attack does not occur if the network uses a long slot time $T_{\text{slot}} = 20$ $\mu$s.

The simulation results are shown in Fig. 4. When the network uses a short slot time, the utilization of node $A_{20}$ jumps when the offered load of the attacker $\rho_1$ exceeds 0.5. Hence, a cascading DoS attack occurs in that case. However, when the network uses a long slot time, the utilization of node $A_{20}$ is not affected. This result confirms that the MAC configuration has an important impact on the possible occurrence of a cascading DoS attack. Because a network using a short slot time has a higher saturated utilization than a network using a long slot time it is more vulnerable to a cascading DoS attack, assuming that all the other parameters are fixed.

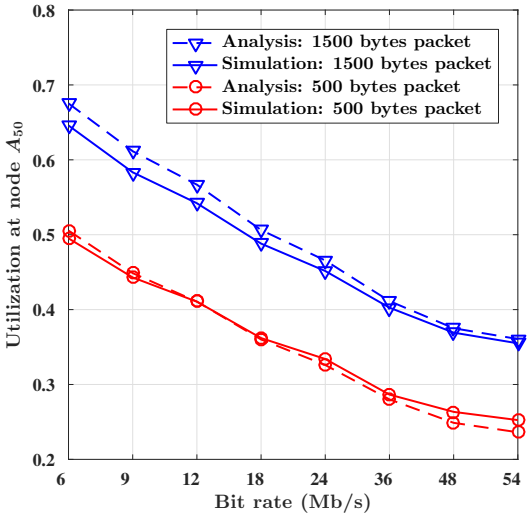
### B. Model accuracy

We next check if the value of the saturated fixed point $\hat{\omega}$, as given by Eq. (17), predicts well the limit of the sequence of node utilizations when the network is saturated. An accurate estimation of $\hat{\omega}$ is crucial for Theorems 1 and 2.

We run ns-3 simulations with 50 pairs of nodes. To ensure that the network is saturated, the offered load $\rho$ is set to 0.98. Fig. 5 depicts the utilization of node $A_{50}$ for different bit rates and packet lengths. Fig. 5(a) shows results for an IEEE 802.11b configuration while Fig. 5(b) shows results for an IEEE 802.11g/n with short slot time. Both figures show excellent match between the analytical and simulation results. In both cases, the saturated utilization decreases with the bit rate but increases with the packet length. This is expected since the overhead of MAC timing parameters remains constant. Likewise, for a given bit rate and packet length, the saturated utilization of IEEE 802.11g/n is higher than that of IEEE




(a) 802.11b.




(b) IEEE 802.11g/n with short slot time.

Fig. 5: Saturated utilization: comparison of analytical and simulation results.

802.11b, due to the lower MAC overhead of IEEE 802.11g/n. While such a property is generally viewed as desirable, it makes a network more vulnerable to a cascading DoS attack as explained previously.

### C. Empirical validation of Theorems 1 and 2

We finally empirically validate our main results, namely that if $\hat{\omega} = \alpha$ then a cascading DoS attack is unfeasible for all traffic loads and the saturation throughput is maximized. To achieve the desired saturated utilization $\alpha$, we compute the theoretically optimal packet length by taking the product of the optimal packet duration given by Eq. (23) with the bit rate.

All our simulations, run for different bit rates and MAC configuration (e.g., IEEE 802.11b and IEEE 802.11g/n), show that no cascading attack occurs when the packet length is set optimally. For instance, for a bit rate of 6 Mb/s, the optimal

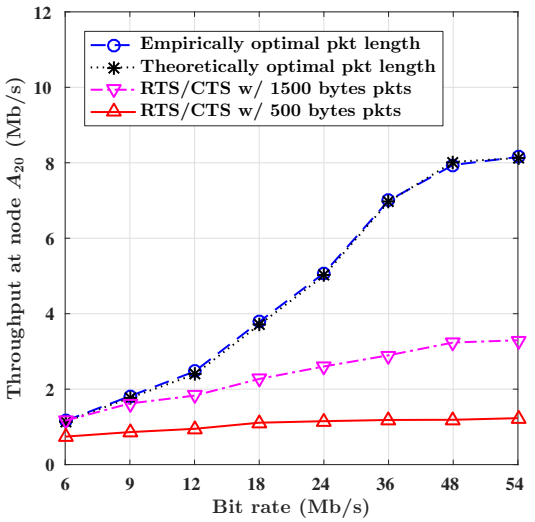



Fig. 6: Comparison of saturation throughput in IEEE 802.11g/n, based on the theoretically optimal packet length, empirically optimal packet length, and RTS/CTS.

packet length is 200 bytes. In that case, Fig. 3, which was introduced in Section III-B, shows that the network experiences a cascading attack if the packet length is 1500 bytes and $\rho = 0.14$. On the other hand, an attacker cannot cause a cascading attack if the packet length is 200 bytes.

Next, we run simulations to evaluate the saturation throughput of the network using the optimal packet length. We set up a saturated network consisting of 20 pairs of nodes with $\rho = 0.98$. We consider a 802.11g/n network using a long slot time. We compare the saturation throughput obtained using the theoretically optimal packet length, based on Eq. (23), with the maximum saturation throughput obtained empirically for 22 different packet lengths, that is, $100, 200, \ldots, 2200$ bytes. We also compare the results when enabling RTS/CTS with packets of length 500 bytes and 1500 bytes.

Figure 6 shows the saturation throughput of node $A_{20}$ at different bit rates. We observe that the saturation throughput obtained using the theoretically optimal packet length is close to the maximum saturation throughput obtained empirically over the 22 different packet lengths. Moreover, the saturation throughput is always higher than that obtained when using RTS/CTS and the difference becomes more significant as the bit rate increases. When the bit rate is 54 Mb/s, the saturation throughput obtained when using the optimal packet length is 2.5 times higher than that obtained when using 1500 bytes packets in conjunction with RTS/CTS.

## VI. Conclusion

In this work, we propose, analyze, and simulate a method to prevent cascading DoS attacks against Wi-Fi networks. When a cascading DoS attack is feasible, a small change in the offered load of the attacker can lead the network to suddenly transition from stability to instability. Our method derives the optimal packet length to prevent such change to ever occur for any

traffic load. Moreover, for the same packet length, we show that the network achieves the maximum saturation throughput performance possible.

Specifically, we provide an analytical model to predict the feasibility of a cascading DoS attack. We develop an iterative analysis that characterizes the sequence of node utilizations, and use fixed point techniques to study its limiting behavior. We show that two types of fixed points may arise: unsaturated fixed points and saturated fixed points. We show that if the saturated fixed point exists, it is unique. We further show that if the value of the saturated fixed point $\hat{\omega}$ is lower or equal to $(3-\sqrt{5})/2 \approx 0.38$, then a cascading attack is unfeasible. In this case, the sequence of node utilizations can only converge to one type of fixed points, no matter what is the initial value of the sequence set by the attacker. The analysis captures the effect of MAC overhead parameters on the feasibility of launching a cascading DoS attack. For instance, with all other parameters kept fixed, we showed that an IEEE 802.11g/n network using a short slot time is more vulnerable to a cascading DoS attack than an IEEE 802.11g/n network using a long slot time.

Our mitigation method simultaneously optimizes the throughput performance of the network. Indeed, the analysis shows that when the saturated utilization is $\hat{\omega} = (3-\sqrt{5})/2$, the network achieves the highest saturation throughput. Our simulation results validates that the throughput performance of the network using the theoretically optimal packet length indeed approaches the highest possible throughput and that it is higher (sometimes significantly) than the throughput obtained using RTS/CTS.

The evaluation of cascading DoS attacks and its mitigation in the latest types of IEEE 802.11 networks represent interesting directions for future work. For instance, the IEEE 802.11ac protocol adds new features, such as MIMO, beamforming, and packet aggregation to improve network efficiency and reduce the impact of MAC overhead. The results of our paper indicate that such features need to be evaluated carefully, since they may have unexpected side effects on neighboring cells and adversely impact an entire network.

## ACKNOWLEDGMENT

This research was supported in part by NSF under grant CNS-1409053.

## REFERENCES

[1] http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html.
[2] https://www.apple.com/homepod/.
[3] https://www.amazon.com/dp/B01E6AO69U.
[4] https://store.google.com/us/product/google_home?hl=en-US.
[5] K. Bicakci and B. Tavli, "Denial-of-service attacks and countermeasures in IEEE 802.11 wireless networks," *Computer Standards & Interfaces*, vol. 31, no. 5, pp. 931–941, 2009.
[6] L. Xin, D. Starobinski, and G. Noubir, "Cascading denial of service attacks on Wi-Fi networks," in *Communications and Network Security (CNS), 2016 IEEE Conference*.
[7] R. Poisel, *Modern communications jamming principles and techniques*. Artech House Publishers, 2011.
[8] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *Communications Surveys & Tutorials, IEEE*, vol. 13, no. 2, pp. 245–257, 2011.
[9] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE Journal on selected areas in communications*, vol. 18, no. 3, pp. 535–547, 2000.
[10] F. Calì, M. Conti, and E. Gregori, "Dynamic tuning of the IEEE 802.11 protocol to achieve a theoretical throughput limit," *IEEE/ACM Transactions on Networking (ToN)*, vol. 8, no. 6, pp. 785–799, 2000.
[11] E. Magistretti, K. K. Chintalapudi, B. Radunovic, and R. Ramjee, "WiFi-Nano: reclaiming WiFi efficiency through 800 ns slots," in *Proceedings of the 17th annual international conference on Mobile computing and networking*. ACM, 2011, pp. 37–48.
[12] X. Sun and L. Dai, "Backoff design for IEEE 802.11 DCF networks: Fundamental tradeoff and design criterion," *IEEE/ACM Transactions on Networking (TON)*, vol. 23, no. 1, pp. 300–316, 2015.
[13] A. Kumar, E. Altman, D. Miorandi, and M. Goyal, "New insights from a fixed-point analysis of single cell IEEE 802.11 WLANs," *IEEE/ACM Transactions on Networking (TON)*, vol. 15, no. 3, pp. 588–601, 2007.
[14] L. Dai and X. Sun, "A unified analysis of IEEE 802.11 DCF networks: Stability, throughput, and delay," *IEEE Transactions on Mobile Computing*, vol. 12, no. 8, pp. 1558–1572, 2013.
[15] C. H. Foh and J. W. Tantra, "Comments on IEEE 802.11 saturation throughput analysis with freezing of backoff counters," *IEEE Communications Letters*, vol. 9, no. 2, pp. 130–132, 2005.
[16] A. Duda *et al.*, "Understanding the performance of 802.11 networks." in *PIMRC*, vol. 8, 2008, pp. 2008–1.
[17] C.-C. Chen, H. Luo, E. Seo, N. H. Vaidya, and X. Wang, "Rate-adaptive framing for interfered wireless networks," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*. IEEE, 2007, pp. 1325–1333.
[18] S. Ray, D. Starobinski, and J. B. Carruthers, "Performance of wireless networks with hidden nodes: A queuing-theoretic analysis," *Computer Communications*, vol. 28, no. 10, pp. 1179–1192, 2005.
[19] I. Broustis, J. Eriksson, S. Krishnamurthy, and M. Faloutsos, "Implications of power control in wireless networks: A quantitative study," *Passive and Active Network Measurement*, pp. 83–93, 2007.
[20] S. Ray, J. B. Carruthers, and D. Starobinski, "RTS/CTS-induced congestion in ad hoc wireless LANs," in *Wireless Communications and Networking, WCNC 2003.*, vol. 3. IEEE, pp. 1516–1521.
[21] K. Xu, M. Gerla, and S. Bae, "Effectiveness of RTS/CTS handshake in IEEE 802.11 based ad hoc networks," *Ad hoc networks*, vol. 1, no. 1, pp. 107–123, 2003.
[22] https://www.nsnam.org/doxygen/classns3_1_1_wifi_remote_station_manager.html#details.
[23] "Different Wi-Fi protocols and data rates," https://www.intel.com/content/www/us/en/support/network-and-i-o/wireless-networking/000005725.html, 2017.
[24] https://www.nsnam.org/doxygen/wifi-mac_8cc_source.html.
[25] M. Gast, *802.11 wireless networks: the definitive guide*. " O'Reilly Media, Inc.", 2005.
[26] "The network simulator ns-3," https://www.nsnam.org/.
[27] M. S. Afaqui, E. Garcia-Villegas, E. Lopez-Aguilera, G. Smith, and D. Camps, "Evaluation of dynamic sensitivity control algorithm for ieee 802.11 ax," in *Wireless Communications and Networking Conference (WCNC), 2015 IEEE*. IEEE, 2015, pp. 1060–1065.
[28] L. Kleinrock, *Queueing systems, Vol. 1*. Wiley, New York, 1975.
[29] L. Kleinrock and F. Tobagi, "Packet switching in radio channels: Part I–Carrier sense multiple-access modes and their throughput-delay characteristics," *IEEE transactions on Communications*, vol. 23, no. 12, pp. 1400–1416, 1975.
[30] S. M. Ross, *Stochastic processes*. Wiley, New York, 1996.
[31] D. Szecsei, *Calculus*, ser. Homework helpers (Career Press Inc.). Pompton Plains, N.J.: Career Press, 2007.