Countering Cascading Denial of Service Attacks on Wi-Fi Networks

Liangxiao Xin, *Member, IEEE,* and David Starobinski, *Senior Member, IEEE*

Abstract—Recent work demonstrates that IEEE 802.11 networks are vulnerable to cascading DoS attacks, wherein a single node can remotely and suddenly congest an entire network. In this paper, we propose, analyze, simulate, and experimentally verify a counter-measure against such attacks. Our main idea is to optimize the duration of packet transmissions in order to weaken coupling effects between neighboring pairs of nodes. Toward that end, we propose a new theoretical model that relates the utilization of neighboring pairs of nodes using a sequence of iterative equations. The model captures important specifications of the IEEE 802.11 MAC layer. Through a fixed point analysis of the sequence, 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 the analysis through extensive ns-3 simulations and demonstrate the effectiveness of the mitigation through experiments with real Wi-Fi cards. A key insight is that IEEE 802.11 networks with relatively large MAC overhead are less susceptible to cascading DoS attacks than networks with smaller MAC overhead.

Index Terms—DoS, IEEE 802.11, hidden nodes, countermeasures.

1 Introduction

IEEE 802.11 standards (Wi-Fi) define wireless communication protocols that allow users to communicate over the unlicensed 2.4 GHz and 5 GHz bands. Wi-Fi enables ubiquitous access to the Internet and has become the most popular local access network technology. According to statistics provided by the Cisco Visual Networking Index 2017 [1], 42% of the Internet traffic in 2015 was transmitted through Wi-Fi. This number is expected to increase to 49% by 2020. Likewise, the number of Wi-Fi hotspots is expected to grow six-fold between 2016 and 2021, from 94.0 millions to 541.6 millions. Therefore, Wi-Fi represents a critical infrastructure for Internet access, and protecting this infrastructure against Denial-of-Service (DoS) attacks is of paramount importance.

Recent work [2] demonstrates a new and particularly dangerous 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 as illustrated in Fig. 1. A receiver (denoted R_x) is within the range of a transmitter (T_x) and a hidden node. Since the transmitter and the hidden node cannot sense each other, collisions happen when they transmit simultaneously, and as a result node T_x must retransmit. Using interference coupling, an attacker, e.g., the hidden node in cell 1, locally raises the amount of traffic that it generates which affect its neighboring cells, e.g., cell 2. Retransmissions by nodes in cell 2 in turn affect nodes in other 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 under both infrastructure and ad-hoc settings. Moreover, the attack can be launched remotely and is protocol compliant, which makes it difficult to locate and identify the attacker. Given the serious consequences of cascading DoS attacks, it is important to find methods to counter them.

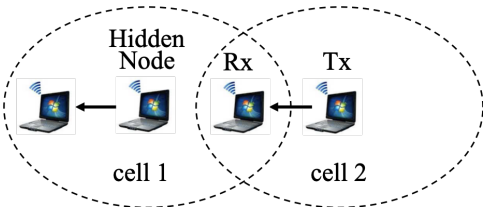


Fig. 1: Interference coupling due to hidden node problem.

In this paper, we propose and evaluate a method to mitigate cascading DoS attacks on Wi-Fi networks. Our key idea is to optimize the durations of packet transmissions (or, equivalently, the packet length divided by the bit rate) to ensure that interference coupling does not propagate and amplify across the network. We propose a new theoretical model where we relate the utilization of nodes in neighboring cells using iterative equations. The model accounts for the impact of MAC overhead, and in particular MAC timing parameters. 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 maximize the saturation throughput. Third, we validate the analytical results using ns-3 simulations. We show the feasibility of launching a cascading

• *L. Xin, and D. Starobinski are with the Division of Systems Engineering, Boston University, Boston, MA 02215 USA (e-mail: xlx@bu.edu; staro@bu.edu).*

attack in a non-linear network, namely an office building model with cross network traffic, and the effectiveness of our proposed mitigation. Fourth, we verify the effectiveness of the mitigation on an experimental testbed equipped with real Wi-Fi cards. A key insight from our work 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 2, we discuss related work and necessary background on the IEEE 802.11 standard. In Section 3, we explain how cascading DoS attacks operate and the impact of the packet length on the feasibility of launching such attacks. In Section 4, 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 5. We evaluate the effectiveness of the mitigation in a real Wi-Fi network in Section 6. We conclude the paper in Section 7. The Appendix contains proofs of Lemmas 4 and 5, and a table of notations.

An earlier, shorter version of this work appears in [3]. This paper primarily differs by providing a new section with experimental results, new simulation results for a network with cross traffic, and complete proofs of all the mathematical results.

2 Related Work and Background

2.1 Related work

The goal of a DoS attack is to impair network services. Traditional jamming attacks [4] 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 [5]. 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 [2] theoretically and empirically demonstrates a cascading DoS attack in Wi-Fi networks. The analysis in [2] 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 [2]). 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 [6], [7], [8], [9], [10], [11], [12], [13]. In particular, an analysis carried out in [13] 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 [14], [15], [16], though none of these works consider security ramifications. The work in [14] shows that coupling causes nodes to transmit at low bit rates, thus aggravating packet losses. The work in [15] 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 throughput of a network where nodes are all saturated (i.e., their queues are never empty) is referred to as *saturation throughput*. The seminal work of Bianchi [6] introduces a simple Markov chain model to estimate the saturation throughput of a single-cell network under ideal channel conditions. The work in [17] extends that analytical model to incorporate the impact of hidden nodes. The saturation throughput in scenarios with non-ideal channel conditions is also studied in [18], [19].

The work in [16] 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].

The evaluation of cascading DoS attacks and its mitigation in the latest types of IEEE 802.11 networks, such as IEEE 802.11ac/ad/ax, is not considered in this paper but represents an interesting direction 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 findings 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.

As an example, IEEE 802.11ac/ad/ax support beamforming, which allows node to perform directional transmissions [22], [23]. A directional signal beam improves spatial reuse since only nodes in the signal direction can sense the signal. Nodes outside the signal beam can transmit at the same time since they do not sense the channel busy. However, this property also introduces the risk that those nodes are hidden [23], [24]. Moreover, IEEE 802.11ad is susceptible to "beam stealing" attacks, where remote attackers may interfere with the beam training procedure and steer the beam of victims toward another direction [25]. Hence, determining whether cascading attacks are feasible in such networks is an interesting open problem.

The latest IEEE 802.11ax protocol introduces the MU-RTS/CTS procedure to protect multi-user (MU) orthogonal frequency division multiple access (OFDMA) transmissions from hidden nodes [26]. An Access Point (AP) successfully reserves a transmission opportunity (TXOP) for MU-OFDMA transmissions if it receives a CTS frame from *any* solicited station after sending a MU-RTS frame. That is, the CTS frame may not be responded by all the

solicited stations. For instance, if a solicited station senses interference due to hidden nodes with respect to the AP, it does not respond to the CTS frame. Thus, the AP will still arrange transmissions for these stations after the MU-RTS/CTS exchange, resulting in wasted channel resource allocation during the TXOP [27]. Moreover, IEEE 802.11ax frames cannot be decoded by legacy devices, which may cause improper behaviour of the virtual carrier sense procedure on those devices [28]. Therefore, hidden nodes can still arise and have detrimental effect in IEEE 802.11ax networks.

Finally, we note that it may be possible to launch cascading attacks on newer Wi-Fi devices through "downgrade attacks." Indeed, some IEEE 802.11 cards downgrade to 802.11b/g when transmitting at low bit rates. Thus, the work in [2] shows an experiment where IEEE 802.11n Wi-Fi cards downgrade to the IEEE 802.11b protocol during a cascading attack.

2.2 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 1 retransmission attempt, the contention window is given by

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

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_{slot}. In all the scenarios considered in this paper, each transmitter is a hidden node with respect to another transmitter. Thus, none of the transmitters can sense transmissions by other nodes. As a result, the backoff counter of each transmitter keeps counting down and never freezes. Accordingly, the average backoff delay at the rth retransmission attempt is

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

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 rth retransmission attempt is

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

TABLE 1: IEEE 802.11 parameters [32]

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

where T_{DIFS} and T_{SIFS} represent respectively the durations of the DIFS and SIFS intervals and T_{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 rth retransmission attempt is

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

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 $R = 7$ [29].

The IEEE 802.11 standard has several variants, which differ in their physical and MAC layer specifications [30]. These variants support transmissions at different bit rates going up 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 [30].

Table 1 shows settings of the timing parameters of IEEE 802.11b 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., $T_{\text{slot}} = 20$ μs) or a short slot time (i.e., $T_{\text{slot}} = 9$ μs) [31]. The long slot time is typically used in a mixed environment composed of both 802.11b and 802.11g/n nodes.

3 Cascading DoS Attacks

3.1 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 [2]. Figure 2 depicts the configuration. The ith pair is denoted (A_i, B_i), where i 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 2.2.

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

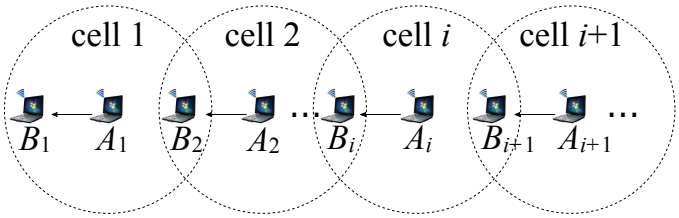


Fig. 2: Network configuration. The dotted circles represent the communication range of nodes A_i. Nodes A_i transmit packets to nodes B_i $(i = 1, 2, \ldots)$. Each transmission pair (A_i, B_i) belongs to a different cell. Nodes A_i are hidden nodes with respect to nodes A_{i+1}.

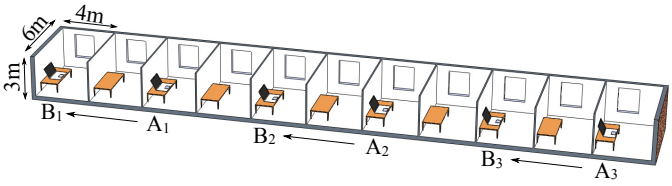


Fig. 3: Example of an attack in an office building. Three transmission pairs (A_i, B_i), where i 2 f1, 2, 3g, are positioned as shown in the figure.

number of retransmissions for each packet. The increased number 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).

3.2 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 ρ_i as the *exogenous 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, 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 3, we consider communication within an office building using the ns-3 building model [33]. The external wall of the building is made of concrete with windows. The internal wall loss is 12 dB [34]. 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 3. Each transmitting node uses a short slot time (i.e., $T_{\text{slot}} = 9$ μs) and a bit rate of 6 Mb/s. The exogenous load at nodes A_2 and A_3 is set to 0.14 while the attacker A_1 varies its load ρ_1. We run simulations of this configuration using the ns-3 simulator [33]. 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 4. 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 exogenous 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 throughput of node A_3. This result holds no matter what packet length is used by the attacker.

The work of [2] only considers the impact of the traffic load and the retry limit on the feasibility of a cascading attack. Figure 4 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.

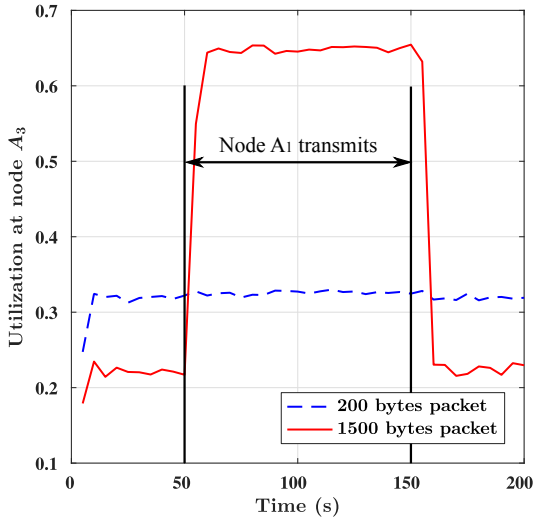
4 Mitigation of Cascading Attacks: Model and Analysis

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 exogenous 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. 2. 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.

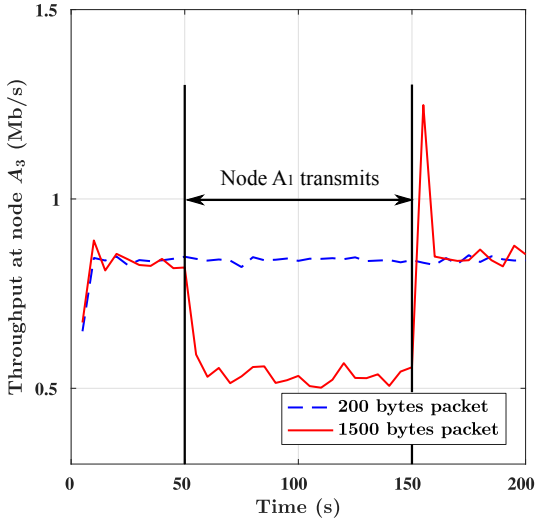
4.1 Model and assumptions

We now present our model, notation, and assumptions. We denote by λ_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 2). The duration of a packet transmission is T (we assume a fixed bit rate). The exogenous load at node A_1 is $\rho_1 = \lambda_1 T$ and the exogenous load at all the other nodes is $\rho = \lambda T$.

The probability that a packet transmitted by node A_i collides is denoted p_i. 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 the original transmission is included in $\overline{r}_i$, hence 1 $\overline{r}_i$ R. That is, when $\overline{r}_i = 1$, packets transmitted by node A_i never collides. When $\overline{r}_i = R$, all the packets collide and reach the retry limit. Note that $\overline{r}_1 = 1$



(a) Utilization.



(b) Throughput.

Fig. 4: 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.

because there is no hidden node that causes packet collisions at node A_1, and packet collisions are the only cause of packet loss in our model.

Finally, we denote by C_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 p_i, $\overline{r}_i$, and C_i.

The utilization of node A_i (i.e., the fraction of time during which it transmits) is denoted u_i. If $\overline{r}_i\lambda_i < C_i$, then the queue of node A_i is stable and by Little's Law [35] its utilization is $\overline{r}_i\lambda_i T$. On the other hand, If $\overline{r}_i\lambda_i > C_i$, then the queue of node A_i is unstable and its utilization is $C_i T$. We refer to $C_i T$ as the *saturated utilization*. Hence, the utilization of node A_i (i 1) is

$$u_i = \min\{\overline{r}_i\lambda_i T, C_i T\}. \quad (5)$$

In order to render the analysis of this queueing network tractable, we make use of Kleinrock's random look assumption [36], 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 $\min\{\overline{r}_i\lambda_i, C_i\}$.

We emphasize that beside these approximations, the rest of the analysis is exact.

4.2 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 $\overline{r}_i$.

Lemma 1. For i 2,

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

Proof: 1) Suppose node A_i starts transmitting a packet at time $t = 0$. According to Assumption 2, the transmission state of node A_{i-1} at time $t = 0$ is the same as at any random point of time due to the Poisson Arrivals See Time Averages (PASTA) property [37]. If node A_{i-1} is transmitting at time $t = 0$, which occurs with probability u_{i-1}, the packet of node A_i collides. If node A_{i-1} is not transmitting at time $t = 0$, then a collision occurs if node A_{i-1} starts transmitting a packet during the interval $[0, T]$. The packet transmission (service) rate of node A_{i-1} is $\min\{\overline{r}_{i-1}\lambda_{i-1}, C_{i-1}\}$. Therefore, the probability that node A_{i-1} starts transmitting a packet during the interval $[0, T]$ is $(1 - e^{-\min\{\overline{r}_{i-1}\lambda_{i-1}, C_{i-1}\}T}) = (1 - e^{-u_{i-1}})$ since the time between consecutive transmission events follows an exponential distribution. We therefore obtain

$$\begin{aligned} p_i &= 1 - u_{i-1} + (1 - e^{-u_{i-1}})(1 - u_{i-1}) \\ &= 1 - e^{-u_{i-1}}(1 - u_{i-1}). \end{aligned}$$

2) The number of transmissions per packet at node A_i is a random variable with mean $\overline{r}_i$. Based on Assumption 1, a packet is either transmitted successfully after $1 \le r \le R$ retransmissions, which occurs with probability $(1 - p_i)\, p_i^{r-1}$, or dropped after R failed retransmissions, which occurs with probability p_i^R. Thus, the average retry count at node A_i is

$$\begin{aligned} \overline{r}_i &= \sum_{r=1}^{R} r(1 - p_i)p_i^{r-1} + p_i^R \\ &= \sum_{r=1}^{R} p_i^{r-1}. \end{aligned}$$

□

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

Lemma 2. Let i 2 and suppose that the queue of node A_i is stable. Then its utilization is

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

Proof: Based on (6) and (7), the utilization of node A_i ($i \geq 2$) is

$$\begin{aligned}\overline{r}_i \lambda T &= \lambda T \sum_{r=1}^{R} (1 - e^{-u_i u_{i-1}})(1 - u_i u_{i-1})^{r-1} \\ &= \rho \sum_{r=1}^{R} (1 - e^{-u_i u_{i-1}})(1 - u_i u_{i-1})^{r-1}.\end{aligned}$$

□

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

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

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 [38], 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 rth 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

$$\sum_{r=1}^{R} p_i^{r-1} T. \tag{9}$$

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

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

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:

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

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

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

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

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

4.3 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. Note that a key difference between the analysis conducted in our paper and [2] is that we develop a method to characterize the saturated utilization (see Lemma 3). Practically, the saturation utilization of a node is smaller than 1 because the node has to spend time on channel contention before transmitting. There exists time between two consecutive packet transmissions where the node is not transmitting. Therefore, the structure of the iterative sequence (see Eq. (14)) and the analysis of its limits are markedly different from the results derived in [2].

Consider the possible limits of the utilization sequence $\{u_i\}_{i=1}^{1}$. 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

$$\omega = \min\{U(\omega), S(\omega)\}. \tag{15}$$

We next define the two possible types of fixed points.

Definition 2 (Saturated and unsaturated fixed points). Let

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

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

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

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 $\{u_i\}_{i=1}^{1}$ is an unsaturated fixed point $\breve{\omega}$. Otherwise, if the limit of the utilization sequence $\{u_i\}_{i=1}^{1}$ 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 exogenous load ρ, (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 $\hat{\omega} \quad (3 \quad \sqrt{5})/2$, then (15) has only one type of fixed points for each traffic load ρ and a cascading DoS attack is unfeasible. In Section 4.6, we further show that if $\hat{\omega} = (3 \quad \sqrt{5})/2$, then the network achieves the highest possible saturation throughput.

4.4 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.

To prove this result, we use the following lemmas (see proofs in Appendix A and B).

Lemma 4. If $b \quad a$, then the function $f(x) = \frac{a+xb}{1+x}$ is monotonically increasing in x.

Lemma 5. Consider an arbitrary sequence $\{a_r\}_{r=1}^{R}$ such that $a_{r+1} \quad a_r$. If $p' > p$. then $\frac{\sum_{r=1}^{R}(p')^{r \ 1}a_r}{\sum_{r=1}^{R}(p')^{r \ 1}} \quad \frac{\sum_{r=1}^{R}(p)^{r \ 1}a_r}{\sum_{r=1}^{R}(p)^{r \ 1}}$.

Based on the above two lemmas, we present the following theorem to show the uniqueness of the value of $\hat{\omega}$.

Lemma 6. Eq. (17) has a unique solution $\hat{\omega}$.

Proof: We show that the function $F(\omega) \ , \ S(\omega) \quad \omega$ 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 [39], there exists a unique solution $F(\hat{\omega}) = 0$ (i.e., $S(\hat{\omega}) = \hat{\omega}$).

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

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

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

$$F(1) = S(1) \quad 1 < 0.$$

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

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

The derivative of $P(\omega)$ is

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

We next prove that $\frac{dS(\omega)}{dP(\omega)}$ is negative for all $\omega \in [0, 1]$, which proves the result. That is, $S(\omega)$ decreases as $P(\omega)$ increases.

Since $S_\omega \quad 0$, the function $S(\omega)$ is decreasing if and only if $S(\omega)^{\ 1}$ is increasing. We thus investigate $S(\omega)^{\ 1}$ which is

$$\begin{aligned} & S(\omega)^{\ 1} \\ = & \frac{\sum_{r=0}^{R \ 1}(P(\omega))^r(d_{s,r}(1 \quad P(\omega)) + d_{f,r}P(\omega) + T)}{\sum_{r=0}^{R \ 1}(P(\omega))^r T} \\ = & \frac{\sum_{r=0}^{R \ 1}(P(\omega))^r d_{s,r}}{\sum_{r=0}^{R \ 1}(P(\omega))^r T} \\ & + \frac{\sum_{r=0}^{R \ 1}(P(\omega))^{r+1}(d_{f,r} \quad d_{s,r})}{\sum_{r=0}^{R \ 1}(P(\omega))^r T} + 1. \end{aligned} \tag{18}$$

The above equation shows that $S(\omega)^{\ 1}$ can be divided into three terms, $\frac{\sum_{r=0}^{R \ 1}(P(\omega))^r d_{s;r}}{\sum_{r=0}^{R \ 1}(P(\omega))^r T}$, $\frac{\sum_{r=0}^{R \ 1}(P(\omega))^{r+1}(d_{f;r} \quad d_{s;r})}{\sum_{r=0}^{R \ 1}(P(\omega))^r T}$ and 1. If all those three terms are non-increasing functions of $P(\omega)$ and at least one of them is increasing, then $S(\omega)^{\ 1}$ is increasing with $P(\omega)$. Since the term 1 is a constant, we start with the term $\frac{\sum_{r=0}^{R \ 1}(P(\omega))^{r+1}(d_{f;r} \quad d_{s;r})}{\sum_{r=0}^{R \ 1}(P(\omega))^r T}$. According to (3) and (4), the value of $d_{f,r} \quad d_{s,r}$ is a positive constant. Thus,

$$\frac{\sum_{r=0}^{R \ 1}(P(\omega))^{r+1}(d_{f,r} \quad d_{s,r})}{\sum_{r=0}^{R \ 1}(P(\omega))^r T} = \frac{P(\omega)(d_{f,r} \quad d_{s,r})}{T} \tag{19}$$

which is increasing with $P(\omega)$. We finally investigate the term

$$\begin{aligned} & \frac{\sum_{r=0}^{R \ 1}(P(\omega))^r d_{s,r}}{\sum_{r=0}^{R \ 1}(P(\omega))^r T} \\ = & \frac{\sum_{r=0}^{R \ 1}(P(\omega))^r(T_{\text{DIFS}} + \overline{T}_{\text{backoff},r} + T_{\text{SIFS}} + T_{\text{ACK}})}{\sum_{r=0}^{R \ 1}(P(\omega))^r T}. \end{aligned}$$

Based on Lemma 5, $\frac{\sum_{r=0}^{R \ 1}(P(\omega))^r d_{s;r}}{\sum_{r=0}^{R \ 1}(P(\omega))^r T}$ increases with $P(\omega)$, since $\overline{T}_{\text{backoff},r}$ is an increasing sequence in r and $T_{\text{DIFS}} + T_{\text{SIFS}} + T_{\text{ACK}}$ is a constant. We conclude that $S(\omega)^{\ 1}$ increases as $P(\omega)$ decreases, which proves the result. □

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

$$\hat{\omega} \quad U(\hat{\omega}). \tag{20}$$

Let

$$G(\omega) \ , \ \frac{\rho\omega}{U(\omega)} = \frac{\omega}{\sum_{r=1}^{R}(1 \quad e^{\ \omega(1 \quad \omega)})^{r \ 1}}. \tag{21}$$

The following lemma follows directly from (20) and (21).

Lemma 7. A saturated fixed point exists at $\hat{\omega}$ if and only if $\rho \quad G(\hat{\omega})$.

Proof: We construct a chain of "iff" implications, starting with the statement that the fixed point $\hat{\omega}$ exists. Based on Equation (15), this property holds iff

$$\hat{\omega} \quad U(\hat{\omega}).$$

From (21), this property holds iff

$$\rho \quad \frac{\rho\hat{\omega}}{U(\hat{\omega})} = G(\hat{\omega}).$$

□

The following lemma establishes when an unsaturated fixed point exists.

Lemma 8. An unsaturated fixed point exists if and only if $\rho < \max_{\omega \in [0,\hat{\omega}]} G(\omega)$.

Proof: We prove that the existence of an unsaturated fixed point implies $\rho < \max_{\omega \in [0,\hat{\omega}]} G(\omega)$ and vice-versa. On one hand, suppose an unsaturated fixed point $\breve{\omega}$ exists. According to Definition 2, the unsaturated fixed point $\breve{\omega}$ satisfies

$$\breve{\omega} = min\{U(\breve{\omega}), S(\breve{\omega})\} = U(\breve{\omega}), \tag{22}$$

and the saturated fixed point $\hat{\omega}$ satisfies

$$\hat{\omega} = min\{U(\hat{\omega}), S(\hat{\omega})\} = S(\hat{\omega}). \tag{23}$$

Since Lemma 6 shows that the saturated fixed point $\hat{\omega}$ is unique, we can replace $S(\breve{\omega})$ in (22) by $\hat{\omega}$. We thus have

$$\breve{\omega} = min\{U(\omega), \hat{\omega}\} = U(\omega) < \hat{\omega}. \tag{24}$$

That is, $0 < \breve{\omega} < \hat{\omega}$. Therefore, the traffic load ρ must satisfy

$$\rho = \frac{\rho\breve{\omega}}{U(\breve{\omega})} = G(\breve{\omega}) < \max_{\omega \in [0,\hat{\omega}]} G(\omega). \tag{25}$$

On the other hand, let $\rho < \max_{\omega \in [0,\hat{\omega}]} G(\omega)$. Since $G(0) = 0$, for any $\omega \in [0, \hat{\omega}]$, we have

$$0 < G(\omega) < \max_{\omega \in [0,\hat{\omega}]} G(\omega).$$

In addition, $G(\omega)$ is continuous in the interval $\omega \in [0, \hat{\omega}]$. According to the intermediate value theorem [39], if $\rho \in [0, \max_{\omega \in [0,\hat{\omega}]} G(\omega)]$, then there exists at least one $\omega \in [0, \hat{\omega}]$ such that $\rho = G(\omega)$. From (21), we obtain that $\omega = U(\omega)$ which by definition represents an unsaturated fixed point. □

4.5 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 ρ. Hence, we provide the following lemma.

Lemma 9. 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 7 and 8. 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

$$\alpha = \frac{3 - \sqrt{5}}{2} \approx 0.38. \tag{26}$$

We now state our first main result.

Theorem 1 (Prevention of cascading attacks). A cascading DoS attack is unfeasible if $\hat{\omega} < \alpha$, where $\hat{\omega}$ is the unique solution of (16) and α is given by (26).

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 9. □

The above theorem implies that an attacker cannot launch a cascading DoS attack, if $\hat{\omega}$ is kept sufficiently low. Practically, this can be achieved by using a short packet duration (or packet length). By shortening the packet duration, the ratio of the transmission time to the duration of MAC overhead is reduced and thus keeps the utilization of the network sufficiently low.

4.6 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 $P(\ )$ and $S(\ )$ are defined in Eqs. (11) and (13), respectively. The saturation throughput is therefore given by

$$\begin{aligned} X(\hat{\omega}) &= (1 - P(\hat{\omega}))\ \hat{\omega} \\ &= e^{-\alpha}(1 - \hat{\omega})\ \hat{\omega}. \end{aligned} \tag{27}$$

Eq. (27) 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 α is given by (26).

Proof: Let $\hat{\omega} \in [0, 1]$. According to (27), the derivative of $X(\hat{\omega})$ is

$$X'(\hat{\omega}) = e^{-\alpha}(1 - 3\hat{\omega} + \hat{\omega}^2). \tag{28}$$

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

$$T = \frac{\alpha \sum_{r=1}^{R} (P(\alpha))^r (d_r^{(s)}(1 - P(\alpha)) + d_r^{(f)} P(\alpha))}{(1 - \alpha) \sum_{r=1}^{R} (P(\alpha))^r}. \tag{29}$$

According to (29), 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 1 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.

Note that for any bit rate, the optimal packet length can be found by multiplying the optimal packet duration with the bit rate. Specifically, denote the optimal packet length by L and the bit rate by b. The optimal packet length is

$$L = T\ b, \tag{30}$$

where T is given by Eq. (29). This setting both maximizes the saturation throughput and prevents a cascading attack (by Theorems 1 and 2).

5 Simulation Results

We next present simulation results using ns-3 [33]. 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 3.2). We then validate the accuracy of our analytical model in predicting the saturated utilization of a network. Next, 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. Finally, we verify the feasibility of the attack and effectiveness of the mitigation in a network with cross-traffic. 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.

5.1 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. 2). Each node A_i transmits 1500 bytes packets at 6 Mb/s bit rate to node B_i ($i = 1, 2, \ldots, 20$). The exogenous load of nodes A_i (i 2) is set to $\rho = 0.14$. Note that 1500 bytes represent the standard IP packet length. Moreover, we know from Fig. 4 that cascading DoS attacks for such a packet length are feasible.

The simulation results are shown in Fig. 5. When the network uses a short slot time, the utilization of node A_{20} jumps when the exogenous load of the attacker ρ_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.

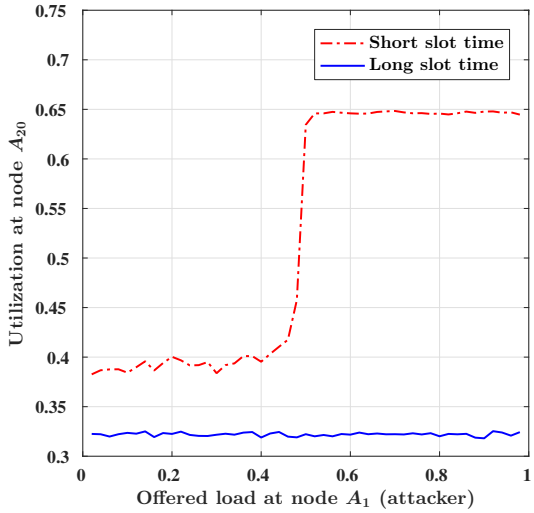


Fig. 5: IEEE 802.11g/n networks under different MAC configurations. With a short slot time $T_{\text{slot}} = 9\ \mu$s, a cascading DoS attack occurs. However, the attack does not occur if the network uses a long slot time $T_{\text{slot}} = 20\ \mu$s.

5.2 Model accuracy

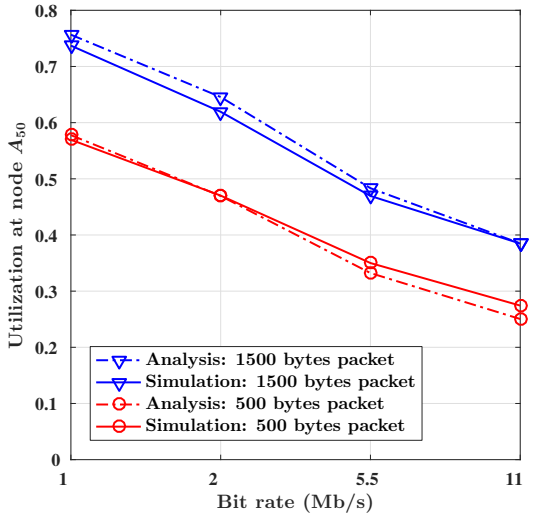
We next check if the value of the saturated fixed point $\hat{\omega}$, as given by Eq. (17), predicts well the limit of the sequence of node utilizations when the network is saturated. An accurate estimation of $\hat{\omega}$ is crucial for Theorems 1 and 2.

We run ns-3 simulations with 50 pairs of nodes. To ensure that the network is saturated, the exogenous load ρ is set to 0.98. Fig. 6 depicts the utilization of node A_{50} for different bit rates and packet lengths. Fig. 6(a) shows results for an IEEE 802.11b configuration while Fig. 6(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 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.

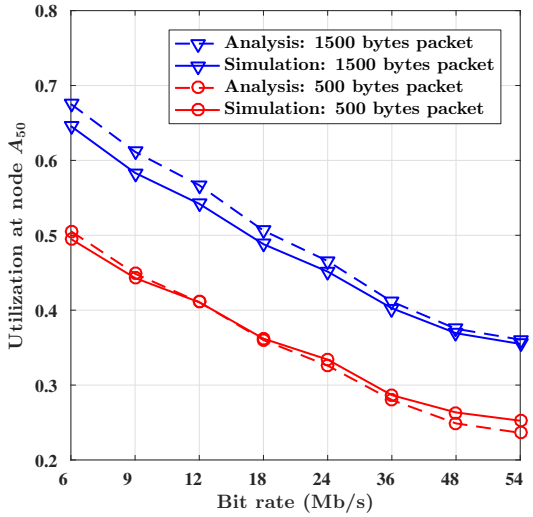
5.3 Empirical validation of Theorems 1 and 2

We next empirically validate our key 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 α, we compute the theoretically optimal packet length by taking the product of the optimal packet duration given by Eq. (29) 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 packet length is 200 bytes. In that case, Fig. 4, which was introduced in Section 3.2, shows that the network experiences a cascading attack if the packet length is 1500



(a) 802.11b.



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

Fig. 6: Saturated utilization: comparison of analytical and simulation results.

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. (29), 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 7 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.

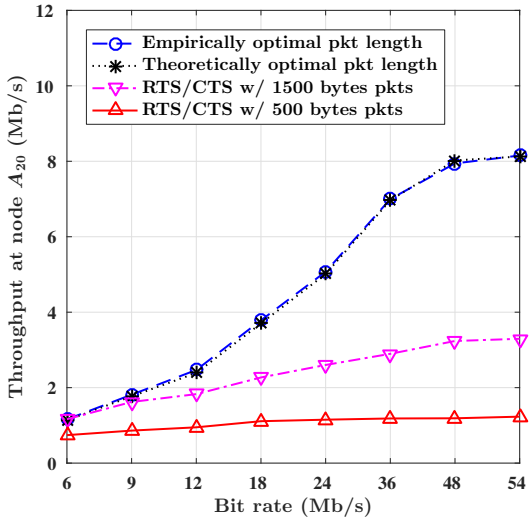


Fig. 7: Comparison of saturation throughput in IEEE 802.11g/n, based on the theoretically optimal packet length, empirically optimal packet length, and RTS/CTS.

5.4 Topology with cross traffic

We next present simulation results to evaluate the effectiveness of the attack and its mitigation in an office building with cross network traffic. Specifically, we assume the presence of additional pairs of communicating nodes in the network besides those directly impacted by the attack. We use the same ns-3 building model as in Section 3.2. As shown in Figure 8, we consider one floor of an office building with rooms arranged along three rows, where each row consists of 11 rooms. To identify the location of a room, we use the coordinates (x, y) where $x \in \{0, 1, 2\}$ and $y \in \{0, 1, \ldots, 10\}$.

We consider a cascading attacks on three transmission pairs (A_i, B_i), $i \in \{1, 2, 3\}$, which are positioned in every other room of the middle row. Node A_1 is the attacker and the other two pairs are victims. Additionally, there are four other transmission pairs (C_j, D_j), $j \in \{1, 2, 3, 4\}$. The transmitters C_j are located in rooms $(0, 2)$, $(0, 6)$, $(2, 4)$, $(2, 8)$ and their receivers D_j are located in rooms $(0, 4)$, $(0, 8)$, $(2, 2)$, $(2, 6)$, respectively. We vary the exogenous load of node A_1 and set the exogenous load of nodes A_2 and A_3 to 0.12 and of nodes C_j to 0.06 for all $j \in \{1, 2, 3, 4\}$. All the nodes transmit UDP packets at 6 Mb/s bit rate. The running time of each simulation is 200 s.

We first set the packet length to 1500 bytes and illustrate the feasibility of the cascading attack in Figure 9. We observe that as node A_1 starts to transmit after 50 s, the utilization of node A_3 jumps from 0.2 to 0.45 while its throughput drops from 0.73 Mb/s to less than 0.6 Mb/s. The utilization and throughput of node A_3 recover once node A_1 stops transmitting after 150 s. This results show a cascading attack is feasible in this simulation. Note that if the load of nodes

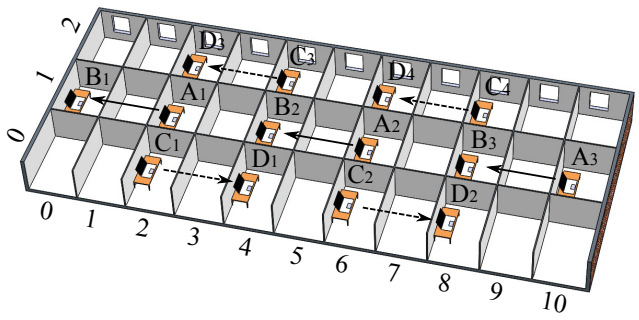


Fig. 8: Network topology with cross traffic. Node A_1 is the attacker, node A_2 and A_3 are victims. Node C_1, C_2, C_3, and C_4 generate cross-traffic.

A_2 and A_3 were set to a much higher (respectively, lower) value, then these nodes would always be saturated (resp., unsaturated), irrespective of the load of node A_1.

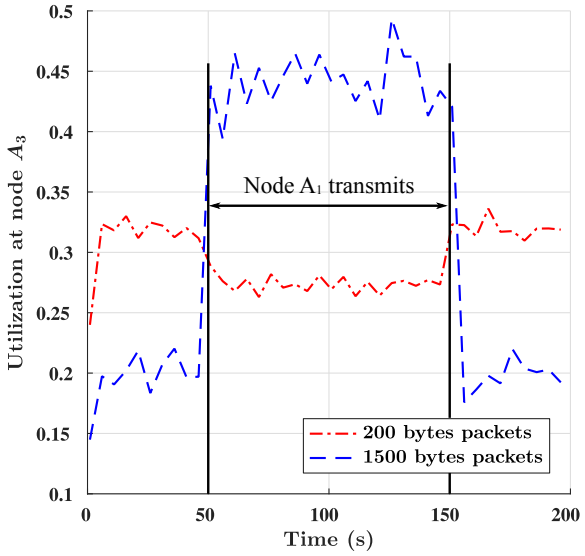
We next demonstrate the effectiveness of the mitigation by changing the packet length to 200 bytes. When node A_1 is transmitting, we observe that the utilization of node A_3 does not increase (in fact, it even slightly decreases) as shown in Figure 9(a). Meanwhile, the throughput of node A_3 is not affected as shown in Figure 9(b). This result shows that cascading attacks are still feasible in a topology with cross traffic and that our proposed mitigation is still effective.

6 Attack and Mitigation in Experimental Testbed

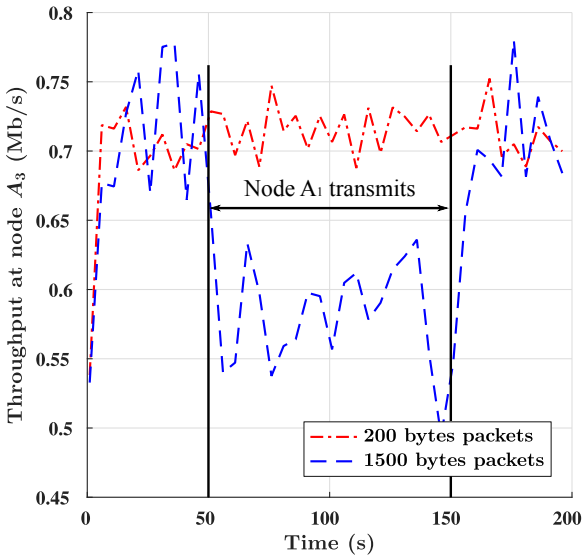
In this section, we provide experimental results to show that shortening packet lengths can prevent the occurrence of a cascading attack in a Wi-Fi network. We perform two experiments with the same parameter settings, except for the packet length. When nodes in the testbed use long packets, a cascading attack is feasible. However, the attack disappears when nodes use short packets.

We set up an experimental testbed as shown in Figure 10. We establish an IEEE 802.11n ad hoc network consisting of three transmission pairs (A_i, B_i), where $i \in \{1, 2, 3\}$. Each node A_i or B_i consists of a PC and a TP-LINK TL-WN772N Wi-Fi USB adapter. We use RF cables to link the nodes and use splitters to split and combine the Wi-Fi signals. As shown in the figure, we add 60 dB attenuators on the links (A_i, B_{i+1}) and 70 dB attenuators on the links (A_i, B_i). The transmission power of all the nodes is set to 0 dBm. Thus, node A_i is a hidden node with respect to node A_{i+1}. We note that at each node B_i, the received signal (interference) strength from the hidden node A_{i-1} is stronger than the signal strength from node A_i. This ensures that an interference caused by hidden node A_{i-1} corrupts any on-going packet transmissions between A_i and B_i at all bit rates.

Our goal is to test whether traffic increase on the link (A_1, B_1) affects the throughput of the link (A_3, B_3). We note that the links (A_1, B_1) and (A_3, B_3) do not interfere directly with each other. If we observe that the throughput of the link (A_3, B_3) drops as traffic increases on the link (A_1, B_1), then we conclude that a cascading attack is feasible. We stress that although the nodes in the testbed are wired together, they can still receive packets from the outside. Therefore, the experimental results are also affected by cross traffic.



(a) Utilization.



(b) Throughput.

Fig. 9: Cascading attack and its mitigation in a network topology with cross traffic.

According to the mitigation, the optimal packet length depends on the bit rate. However, since the Wi-Fi cards used in the experiments are closed-source, we cannot modify the packet length at different bit rates. Therefore, we set the packet length for the long packet and short packet experiments to 1500 bytes and 500 bytes, respectively.

The results of the experiments are shown in Figure 11. Figure 11(a) depicts the results obtained with long packets. We observe that when node A_1 starts to transmit after 50 s, the throughput of nodes A_2 and A_3 drops from 400 Kb/s to 100 Kb/s. When node A_1 stops transmitting after 100 s, the throughput of nodes A_2 and A_3 recovers.

Next, we set the packet length to 500 bytes and repeat the experiment. As shown in Figure 11(b), transmissions at node A_1 do not have an impact on the throughput of the

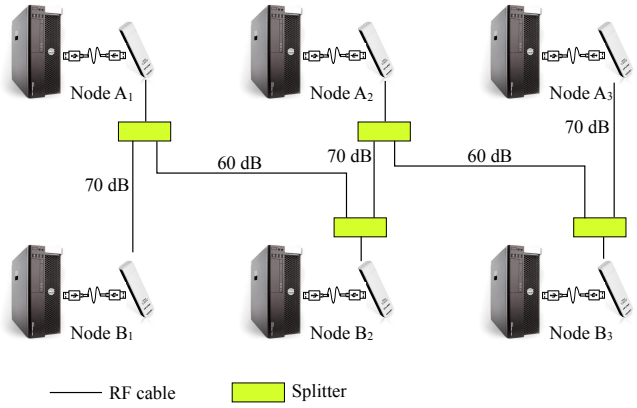


Fig. 10: Experimental testbed.

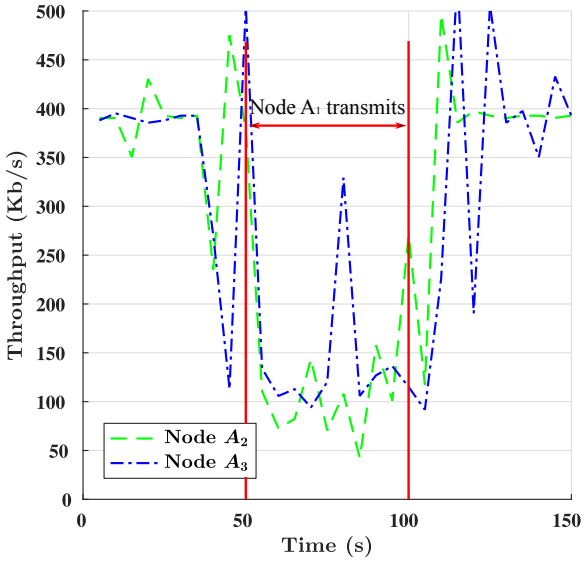
other nodes. This result shows that the attack is feasible when the network transmits 1500 byte-long packets but is unfeasible when the packet length is shortened to 500 bytes. This result shows that shortening the packet length is an effective measure against cascading attacks in a real Wi-Fi setting.

7 Conclusion

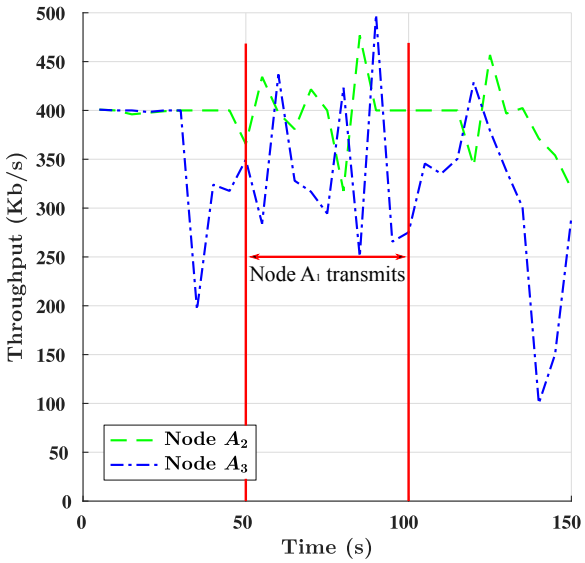
In this work, we propose, analyze, simulate, and experimentally verify a method to prevent cascading DoS attacks against Wi-Fi networks. When a cascading DoS attack is feasible, a small change in the exogenous load of the attacker can lead the network to suddenly transition from stability to instability. 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. For a retry limit $R = 7$, 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



(a) Attack is feasible when nodes transmit 1500 bytes packets.



(b) Attack is unfeasible when nodes transmit 500 bytes packets.

Fig. 11: Feasibility assessment of a cascading DoS attack in the experimental testbed.

throughput and that it is higher (sometimes significantly) than the throughput obtained using RTS/CTS. We also provide simulation results to assess the effectiveness of our method in a network with cross traffic.

Finally, we report experimental results on the feasibility of a cascading attack and its mitigation on a real Wi-Fi network. The results show that the cascading attack is feasible in a practical scenario and that shortening the packet length is an effective way to mitigate the attack.

Acknowledgment

This research was supported in part by NSF under grant CNS-1409053, CNS-1908087, and CNS-2006628.

REFERENCES

[1] http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html.

[2] L. Xin, D. Starobinski, and G. Noubir, "Cascading Denial of Service Attacks on Wi-Fi Networks," in *2016 IEEE Conference on Communications and Network Security (CNS)*, October 2016.

[3] L. Xin and D. Starobinski, "Mitigation of Cascading Denial of Service Attacks on Wi-Fi Networks," in *2018 IEEE Conference on Communications and Network Security (CNS)*, May 2018.

[4] R. Poisel, *Modern communications jamming principles and techniques*. Artech House Publishers, 2011.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] A. Duda *et al.*, "Understanding the performance of 802.11 networks." in *PIMRC*, vol. 8, 2008, pp. 2008–1.

[14] 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.

[15] 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.

[16] 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.

[17] B. Jang and M. L. Sichitiu, "IEEE 802.11 saturation throughput analysis in the presence of hidden terminals," *IEEE/ACM Transactions on Networking (TON)*, vol. 20, no. 2, pp. 557–570, 2012.

[18] Z. Hadzi-Velkov and B. Spasenovski, "Saturation throughput-delay analysis of ieee 802.11 dcf in fading channel," in *Communications, 2003. ICC'03. IEEE International Conference on*, vol. 1. IEEE, 2003, pp. 121–126.

[19] F. Daneshgaran, M. Laddomada, F. Mesiti, M. Mondin, and M. Zanolo, "Saturation throughput analysis of ieee 802.11 in the presence of non ideal transmission channel and capture effects," *IEEE transactions on Communications*, vol. 56, no. 7, 2008.

[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] E. Perahia and M. X. Gong, "Gigabit wireless lans: an overview of ieee 802.11 ac and 802.11 ad," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 15, no. 3, pp. 23–33, 2011.

[23] B. Bellalta, "IEEE 802.11 ax: High-efficiency WLANs," *IEEE Wireless Communications*, vol. 23, no. 1, pp. 38–46, 2016.

[24] J. H. Winters, "Smart antenna techniques and their application to wireless ad hoc networks," *IEEE wireless communications*, vol. 13, no. 4, pp. 77–83, 2006.

[25] D. Steinmetzer, Y. Yuan, and M. Hollick, "Beam-Stealing: Intercepting the Sector Sweep to Launch Man-in-the-Middle Attacks on Wireless IEEE 802.11ad Networks," in *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, ser. WiSec '18, 2018, p. 12–22.

[26] E. Khorov, A. Kiryanov, A. Lyakhov, and G. Bianchi, "A tutorial on IEEE 802.11 ax high efficiency WLANs," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 197–216, 2018.

[27] S.-I. Sou and Y. Lee, "Trigger-based approach with hidden node problem for uplink multi-user transmission in 802.11 ax," in *2017 IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. IEEE, 2017, pp. 1–5.

[28] M. Z. Ali, J. Mišić, and V. B. Mišić, "Impact of hidden nodes on uplink transmission in IEEE 802.11 ax heterogeneous network," in *2018 14th International wireless communications & mobile computing conference (IWCMC)*. IEEE, 2018, pp. 118–123.

[29] https://www.nsnam.org/doxygen/classns3_1_1_wifi_remote_station_manager.html#details.

[30] "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.

[31] https://www.nsnam.org/doxygen/wifi-mac_8cc_source.html.

[32] M. Gast, *802.11 wireless networks: the definitive guide*. " O'Reilly Media, Inc.", 2005.

[33] "The network simulator ns-3," https://www.nsnam.org/.

[34] 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.

[35] L. Kleinrock, *Queueing systems, Vol. 1*. Wiley, New York, 1975.

[36] 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.

[37] R. W. Wolff, "Poisson arrivals see time averages," *Operations Research*, vol. 30, no. 2, pp. 223–231, 1982.

[38] S. M. Ross, *Stochastic processes*. Wiley, New York, 1996.

[39] D. Szecsei, *Calculus*, ser. Homework helpers (Career Press Inc.). Pompton Plains, N.J.: Career Press, 2007.

APPENDIX

.1 Proof of Lemma 4

Proof: Let $b > a$. The derivative of function $f(x)$ is

$$f^{0}(x) = \frac{b(1+x) \quad (a+xb)}{(1+x)^2} = \frac{b \quad a}{(1+x)^2} \quad 0.$$

□

.2 Proof of Lemma 5

Proof: We to prove this lemma by induction. When $R = 2$, we have $\frac{a_1 + pa_2}{1+p}$. Its derivative is

$$(\frac{a_1 + pa_2}{1+p})^{0} = \frac{a_2(1+p) \quad (a_1 + pa_2)}{(1+p)^2} = \frac{a_2 \quad a_1}{(1+p)^2} \quad 0.$$

Thus, when $R = 2$, the lemma is correct. Next, assume the hypothesis holds for $R \quad 2$. That is,

$$\frac{\sum_{r=1}^{R}(p^{0})^{r} \quad {}^{1}a_r}{\sum_{r=1}^{R}(p^{0})^{r} \quad 1} \quad \frac{\sum_{r=1}^{R}(p)^{r} \quad {}^{1}a_r}{\sum_{r=1}^{R}(p)^{r} \quad 1}.$$