ABSTRACT

Recent work shows that an adversary can exploit a coupling effect induced by hidden nodes to launch a cascading attack causing global congestion in a Wi-Fi network. The underlying assumption is that the power of interference caused by a hidden node is an order of magnitude stronger than the signal sent to the receiver. In this paper, we investigate the feasibility of cascading attacks with weakly interfering hidden nodes, that is when the signal-to-interference ratio is high. Through extensive ns-3 simulations, including for an indoor building model, we show that cascading attacks are still feasible. The attacks leverage two PHY-layer phenomena: receiver capture and bit rate adaptation. We show that the attack relies on a coupling effect, whereby the average bit rate of a transmission pair drops sharply as the channel utilization of a neighboring pair gets higher. This coupling effect facilitates the propagation of the attack throughout the network.

Cascading Attacks on Wi-Fi Networks with Weak Interferers

Liangxiao Xin
Boston University
Boston, MA
xlx@bu.edu

David Starobinski
Boston University
Boston, MA
staro@bu.edu

CCS CONCEPTS

• Security and privacy → Denial-of-service attacks; • Networks → Link-layer protocols; Network simulations; Denial-of-service attacks;

KEYWORDS

IEEE 802.11; denial of service; chain reaction; congestion collapse

1 INTRODUCTION

Wi-Fi relies on a distributed access control mechanism, known as carrier-sense multiple access (CSMA) [1], to coordinate channel access among multiple Wi-Fi users to avoid collisions over the shared channel. However, CSMA cannot prevent collisions caused by hidden nodes, which are nodes located outside the sensing range of the sending station but within the communication/interference range of the receiver [9].

Interference caused by hidden node induces a coupling effect between neighboring Wi-Fi cells. Indeed, the presence of a hidden node in one cell causes packet collisions and increased traffic (due to packet retransmissions) in its neighboring cells. This coupling effect can be exploited by an attacker to launch a network-wide, yet protocol-compliant Denial-of-Service (DoS) attack on a Wi-Fi network. This attack is known as a cascading attack [11].

In a cascading attack, an attacker, which is a hidden node, increases the rate at which it generates and transmits packet over its channel. These transmissions affect nodes in neighboring cells, which cause them to increase their own rates of packet transmissions and impact other nodes in other cells. Depending on the network and traffic parameters, this effect may keep amplifying and propagating, resulting in a chain reaction where the entire network gets congested. The work in [11] verifies the feasibility of such attacks through analysis and experiments with Wi-Fi card.

The attack described in [11] assumes that, at the receiver’s end, the power of interference caused by a hidden node is stronger than the power of the signal of the sending station. Due to this assumption, any overlap between transmissions of the station and the hidden node causes a loss of the packet transmitted by the station. In contrast, in this paper, we investigate the case where interference caused by hidden nodes is on the same order or weaker than the signals of sending stations. Our main objective is to find out whether cascading attacks are still feasible in those situations. Through extensive ns-3 simulations, we provide a positive answer to this question.

The attack leverages two phenomena. The first phenomenon is a PHY-layer effect known as receiver capture [7]. Accordingly, if the PHY header of the packet transmitted by the hidden node is decoded first, the packet sent by the station is lost (assuming the two packet transmissions overlap). Thus, even though not all packets transmitted by the station are lost, a large fraction still is.

The second phenomenon relates to bit rate adaptation. Specifically, rate adaptation algorithms vary the bit rate used for packet transmissions based on the observed quality of the channel. While different algorithms have been proposed in the literature [4], most gradually lower the bit rate upon experiencing packet losses. Since packet losses are still possible due the receiver capture effect, rate adaptation algorithms may end up significantly lowering the bit rate of Wi-Fi stations, sometimes down to the base rate of 1 Mb/s. As a result, the capacity of the shared channel is drastically reduced (since each packet transmission uses the shared channel for a longer amount of time) leading to traffic congestion.

The main contributions of this paper can thus be summarized as follows:

(1) We identify and document a coupling effect between neighboring cells, due to hidden nodes and receiver capture. We provide simulations of the packet loss probability with and
without receiver capture. We show that with receiver capture, a packet sent by a station is lost irrespective of the signal-to-interference ratio (SIR) and the bit rate.

(2) Leveraging the above coupling effect, we demonstrate the feasibility of launching cascading attacks on Wi-Fi networks using weak hidden nodes (i.e., hidden nodes producing weak interference). Through extensive ns-3 simulations, including for an indoor building model, we show that the coupling effect may propagate, thus reducing the channel capacity across an entire chain of Wi-Fi cells. These results apply to several rate adaptation algorithms.

2 RELATED WORK

The feasibility of launching a cascading attack on Wi-Fi networks is demonstrated in [10, 11]. These works assume the presence of strong interferers, whereby a transmission by a hidden node always corrupts another on-going packet transmission. In this paper, we show how weak interference by hidden nodes still lead to a coupling effect that can be exploited for launching a cascading attack.

We next explain the differences between the well-known capture effect and the lesser known receiver’s capture effect, which is the focus of our paper. The capture effect pertains to the fact that two overlapping transmissions may not necessarily result in a packet loss. Specifically, if the power of a detected packet exceeds the combined power of interfering signals beyond a certain threshold, then that packet can still be decoded successfully. In Wi-Fi networks, this effect occurs only when the packet with the strongest power is received before others. That is, the packet with the highest power is transmitted first. The works in [5, 6, 8] provide models of Wi-Fi networks integrating the capture effect and show that the packet loss probability can be significantly lower than in models that ignore the capture effect, e.g., Bianchi’s Markov model [3].

Under the receiver capture effect [7], a receiver aligns its state machine with information provided by the PHY header of the first transmission, before the second packet arrives. We stress that the receiver does not need be the intended recipient of the first transmission (because there is no destination address in the PHY header). Under the receiver capture effect, the second transmission (which may be a packet destined to the receiver) cannot be properly decoded and this packet is lost.

3 BACKGROUND

3.1 Physical layer reception

IEEE 802.11 uses the Physical Layer Convergence Procedure (PLCP) to implement physical layer functionalities [1]. The format of a packet at the physical layer consists of a PLCP preamble, a PLCP header and data (payload). When a receiver processes packets at the physical layer, it transits between two PLCP states, the Carrier Sense/Clear Channel Assessment (CS/CCA) state and the Receive (Rx) state. The transitions between those states are illustrated in Figure 1. In the CS/CCA state, the receiver monitors the state of the channel. Once it detects a valid PLCP preamble and header, it moves to the Rx state and processes the payload using information provided in the PLCP header. In particular, using packet length information, the receiver stays in the Rx state until the last bit of the packet is presumably received. Regardless of whether the payload is correctly received or not, the reception ends at that point and the receiver moves back to the CS/CCA state.

3.2 The receiver capture effect

Since the PLCP header only contains radio information, the address of the intended receiver of a packet is unknown until it is checked by the MAC layer. Thus, at the physical layer, a node processes any packet heard from the air. Once the node detects a valid PLCP preamble and header, it moves from the CS/CCA to the Rx state. Therefore, the node cannot detect the PLCP preamble and header of other packets (including those destined to itself) until the current packet reception ends. This phenomenon is known as the receiver capture effect [7].

4 ATTACK SCENARIO

We now describe the attack scenario studied in this paper. Our goal is to assess the feasibility of a chain reaction. Hence, we consider the network topology shown in Figure 2. This topology consists of M single-hop pairs of Wi-Fi nodes. Each pair belongs to a different cell i ∈ (1, 2, . . . , M). In each cell i, node Ai transmits packets to node Bi. The dash circle around each node Ai represents its communication range. We assume that node Bi can sense transmissions from both nodes Ai and Ai−1, but node Ai and node Ai−1 cannot sense each other. Thus, node Ai−1 is a hidden node with respect to node Ai. In this paper, we consider the practical scenario where at node Bi the signal received from the transmitter Ai is stronger than that received from the hidden node Ai−1. In this scenario, the hidden node causes weak interference, but a packet loss is still possible due to the receiver capture effect. We also assume that each node Ai in the topology runs a rate adaptation algorithm, such as ARF, Onoe or AMRR.

The attack proceeds as follows. An adversary that controls node A1 increases its packet generation rate. Though the interference generated by node A1 is weak, it stills leads to packet losses on the link between A2 and B2 due to receiver capture. Hence, node A2 retransmits packets and gradually lowers its bit rate. The lower bit rate prolongs the duration of packet transmissions. Hence, transmissions by node A2 add interference on the link between A3 and B3 which increases the rate of packet losses between A3 and B3 and reduces the bit rate of node A3, and so on.

5 SIMULATIONS

In this section, we run ns-3 simulations of IEEE 802.11g/n networks for the scenario depicted in Figure 2. We define the utilization of node Ai as the average fraction of time during which node Ai
transmits. In addition, we denote by $SIR$ the ratio of the signal strength of node $A_i$ (signal) to the signal strength of node $A_{i-1}$ (interference) observed at node $B_i$.

5.1 Hidden node

Our first simulation evaluates the impact of a hidden node on the packet loss probability for different SIR and bit rates. We consider a network comprising $M = 2$ cells. In each cell $i \in \{1, 2\}$, node $A_i$ sends 1500-byte UDP packets to node $B_i$, $i \in \{1, 2\}$. Thus, node $A_1$ is a hidden node with respect to node $A_2$. We repeat each simulation 10 times and average the results (we also compute 95% confidential intervals, but since they are very narrow, they cannot be seen on the graphs).

We consider two cases:

1. Node $A_1$ starts transmitting a packet right after node $A_2$ finishes transmitting the PLCP preamble and header of a packet.
2. Node $A_2$ starts transmitting a packet right after node $A_1$ finishes transmitting the PLCP preamble and header of a packet.

Figure 3 shows the results for different SIR and bit rates. Case (1) (the curve in blue) corresponds to the classical capture effect. If the SIR is above a certain threshold, the packet transmitted by node $A_2$ is received with high probability by node $B_2$, otherwise it is lost. We note that the threshold is pretty sharp and depends on the bit rate. The higher the bit rate, the higher the SIR needed to successfully receive a packet. For instance, Figure 3 (a) shows that the threshold for a successful reception by $B_2$ at 1 Mb/s is about 0 dB. Figures 3(b), (c), and (d) show that for bit rates of 12 Mb/s, 24 Mb/s, and 54 Mb/s, the SIR threshold for successful reception is about 10 dB, 15 dB, and 25 dB, respectively.

On the other hand, case (2) (the curve in red) corresponds to the receiver capture effect. We observe that a packet transmitted by node $A_2$ is always lost, regardless of the SIR. We conclude that the order of packet arrivals plays a critical role and that a weak hidden node can still induce significant packet losses, even at high SIR.

5.2 Cascading attack in an office building

We next demonstrate the impact of a cascading attack in an IEEE 802.11g/n network comprising $M = 3$ transmission pairs. The network is deployed in an office floor of a building containing 11 rooms, as shown in Figure 4. The physical parameters of the wireless channel are based on the building model [2] of ns-3. The propagation losses between nodes are estimated according to the hybrid buildings propagation loss model [2] of ns-3. The parameter settings of these two models are listed in Table 1.

Each node $A_1$ transmits 1500-byte UDP packets to nodes $B_i$, where $i \in \{1, 2, 3\}$. The retry limit is set to 7. Nodes $A_2$ and $A_3$ generate packets according to Poisson processes with mean rate 0.7 Mb/s. Simulations are run for 600 seconds. Node $A_1$ (the attacker) starts its transmissions after 200 seconds and ends after 400 seconds. When node $A_1$ is active, it generates packets at rate 54 Mb/s, which implies that its transmission queue is never empty.

Figure 5(a) depicts the average bit rate at node $A_3$ for different rate adaptation algorithms, namely ARF, Onoe, and AMRR. In all cases, during the first 200 seconds, node $A_1$ does not transmit. Hence, the bit rate at nodes $A_3$ climbs from its initial value of 1 Mb/s to 54 Mb/s. We note that the bit rate under ARF and Onoe converges faster to 54 Mb/s than under the more conservative AMRR algorithm. Once node $A_1$ starts transmitting, though, the bit rate of $A_3$ drops quickly to low values between 1 and 2 Mb/s for all three algorithms. The reason for the drop are packet retransmissions by node $A_2$ which cause packet loss at node $B_3$ due to the receiver capture effect. These packet losses induce the rate adaptation algorithm at node $A_3$ to lower the bit rate. We stress here that node $B_3$ is outside the interference range of node $A_1$. Hence, this result demonstrates the cascading nature of the attack launched by node $A_1$.

The change of the bit rate at node $A_3$ impact its utilization. Figure 5(b) illustrates this fact. During the first 200 seconds, node $A_1$ does not transmit. We observe that the utilization of node $A_3$ decreases as its bit rate increases. This is because the high bit rate shortens the duration of packet transmissions, which in effect means that the channel capacity is higher from the perspective of node $A_3$. Similarly, when node $A_1$ is transmitting, the utilization...
of node $A_3$ increases reaching values at or above 0.8. This implies that the channel gets congested.

As a consequence of channel congestion, $B_3$ does not receive some UDP packets transmitted by node $A_3$, as shown in Table 2. Specifically, when node $A_1$ transmits, $B_3$ misses about 3% of the UDP packets for Onoe and AMRR, and about 8% of the packets for ARF. Yet, when node $A_1$ is not transmitting, all the UDP packets transmitted by node $A_3$ are received by node $B_3$. These results confirm that cascading attacks with weak interferers are feasible.

**ACKNOWLEDGMENT**

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

**REFERENCES**


