Poster Abstract: Jamming WLAN Data Frames and Acknowledgments using Commodity Hardware

Florian Klingler and Falko Dressler
Heinz Nixdorf Institute and Dept. of Computer Science, Paderborn University, Germany
{klingler,dressler}@ccs-labs.org

***Abstract*—Actively interfering wireless communication (also called jamming) to prevent a potential receiver to decode particular frames has recently attracted much interest in the research community. Reactive jammers extend this concept to allow on-demand selection whether to jam specific frames based on information included in the headers of those particular frames. Recently, several approaches were presented to allow reactive jamming by using commodity hardware, however, with certain limitations, e.g., a minimum necessary frame length. We go one step beyond and, to the best of our knowledge, present a first study on the feasibility of jamming even IEEE 802.11 control frames, such as unicast Acknowledgments (ACKs) following a reactive jamming approach. Our system has been implemented on commodity hardware. We further present analytical timing insights into the possibility of jamming control frames as well as regular data frames.**

I. Introduction

Actively interfering wireless communication, also called jamming, got much attention in the research community recently [1]–[5]. Although many approaches to jam of wireless signals require specialized hardware, e.g., Software Defined Radios (SDRs) [5], prototypes based on commodity hardware [2], [3] or even smartphones [4] have been shown feasible. Besides harmful usage of jammers to prevent a potential receiver from decoding wireless communication, jamming can also be useful for beneficial networking aspects. A good example is Friendly Jamming [3], where a jammer interferes communication of a potential attacker in the network such that receivers cannot be negatively influenced by the attacker. An extension to raw jamming of all wireless communication are *reactive* (or selective) jammers [2]. These types of jammers can decide on-demand and while a frame is being transmitted whether to interfere that particular frame based on information included in the frame. Applications include blocking of particular WLAN networks (see DA/FCC: DA-14-1444), blocking individual transmissions [1], and even delaying network access for many users in vehicular networks [6].

However, the limiting factor of reactive jamming is mainly the time it takes from starting the decoding of a frame and the decision whether to jam or not until the actual generation of the interference signal [2]. In this paper, we investigate this issue by measuring the reaction time for different configurations. Consequently we provide an analytical feasibility study on the minimum frame size and Modulation and Coding Schemes (MCSs) for reactive jamming of regular IEEE 802.11 WLAN data frames and unicast Acknowledgment (ACK) frames.

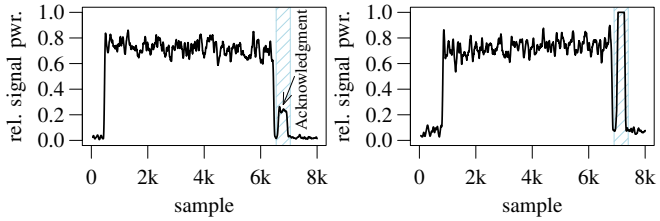
II. Experiment Setup

To evaluate the feasibility of jamming WLAN ACKs, we take advantage of the system proposed by Vanhoef and Piessens [2], which presents driver and firmware enhancements for `ath9k`-based WLAN chipsets to allow jamming of IEEE 802.11 frames. One of the operating principles of the system presented in [2] is that the jamming device (usually a WLAN USB dongle) only decodes the first few bytes of an incoming frame and immediately schedules a jam frame to cause interference.

We extend this system to precisely control the time at which this particular jam frame is transmitted in order to allow generating interference even for control frames such as ACKs of unicast data transmissions as outlined in Figure 1. Such precise time control is beneficial to evaluate, e.g., the impact of lost ACKs on the networking performance [6] or the impact of OFDM interference on IEEE 802.11p [7].

According to our observations, this process is tied to strict timing constraints consisting of (a) t_{detect}, the time of decoding the first bytes of a frame to decide whether to jam that particular frame, and (b) t_{init}, the time it takes to start transmitting the jam frame. Naturally, there exists a lower bound of the frame length, which one is able to jam limited by $t_{\text{detect}} + t_{\text{init}}$. For simplicity, in our evaluations, we only focus on the sum $t_{\text{detect}} + t_{\text{init}}$ and check the first bytes of the IEEE 802.11 frame control field to match a frame to be jammed. We measure the combined delay upon which our jam frame starts being transmitted. This will serve as input for our analytical model to calculate the additional required waiting time to successfully jam unicast ACKs for different data rates and frame lengths.

For our evaluations, we used a pair of PC Engines APU2 devices each outfitted with a *Mikrotik R11e-5HnD* wireless card employing a *AR9582* wireless chip. We configured the devices in IEEE 802.11 WLAN OCB mode on 5.89 GHz running



(a) normal WLAN communication (b) jamming the acknowledgment

Figure 1. Relative signal powers of a unicast data transmission measured on an SDR: Data frame and acknowledgment.

Table I
MEASURED DELAYS BETWEEN DETECTING A WLAN FRAME AND TRANSMITTING A JAM FRAME.

MCS	**BPSK-1/2**	**BPSK-3/4**	**QPSK-1/2**	**QPSK-3/4**
data rate	6 Mbit/s	9 Mbit/s	12 Mbit/s	18 Mbit/s
N_{DBPS}	24	36	48	72
$T_{\text{jam-delay}}$	141 µs	108 µs	90 µs	73 µs
	16-QAM-1/2	**16-QAM-3/4**	**64-QAM-1/2**	**64-QAM-3/4**
	24 Mbit/s	36 Mbit/s	48 Mbit/s	54 Mbit/s
	96	144	192	216
	63 µs	56 µs	51 µs	50 µs

iperf 2 to exchange unicast UDP traffic. Using an SDR, we measure the time $T_{\text{jam-delay}}(N_{\text{DBPS}}) = t_{\text{detect}}(N_{\text{DBPS}}) + t_{\text{init}}$ for different MCSs for a Panasonic N5HBZ0000055 USB WLAN adapter and report the observed values in Table I, where N_{DBPS} denotes the number of bits transmitted per symbol.

III. ANALYTICAL EVALUATION

According to the PLME-TXTIME.confirm primitive outlined in the IEEE 802.11 standard [8], the time it takes to transmit a frame of length l bit is derived as

$$t_{\text{tx}}(l) = T_{\text{preamble}} + T_{\text{signal}} + T_{\text{sym}} \times \left\lceil \frac{16 + l + 6}{N_{\text{DBPS}}} \right\rceil. \quad (1)$$

Specifically, we use parameters based on a 20 MHz bandwidth, that is $T_{\text{preamble}} = 16\,\mu\text{s}$, $T_{\text{signal}} = 4\,\mu\text{s}$, and $T_{\text{sym}} = 4\,\mu\text{s}$.

After each IEEE 802.11 unicast transmission, a sender expects an ACK being transmitted by the receiver after a t_{SIFS}, which corresponds to 16 µs in our configuration. Given an ACK length of $L_{\text{ACK}} = 112\,\text{bit}$ and an arbitrary length L_{DATA} of the unicast frame, we are able to derive a lower and upper bound of waiting time for a jam frame in order to only interfere with the ACK frame as

$$\begin{aligned} t_{\text{jam-lower}} &= t_{\text{tx}}(L_{\text{DATA}}) + t_{\text{SIFS}} - T_{\text{jam-delay}}(N_{\text{DBPS}}) \\ t_{\text{jam-upper}} &= t_{\text{tx}}(L_{\text{DATA}}) + t_{\text{SIFS}} + t_{\text{tx}}(L_{\text{ACK}}) - T_{\text{jam-delay}}(N_{\text{DBPS}}) \\ t_{\text{jam-wait}} &= \left[t_{\text{jam-lower}}, t_{\text{jam-upper}}\right]. \end{aligned} \quad (2)$$

This way we can study the feasibility of jamming ACK frames for different payload lengths and MCSs as outlined in Figure 2. Naturally, whenever the property $t_{\text{jam-upper}} < 0$ holds, it is infeasible to jam the ACK as $T_{\text{jam-delay}}$ already exceeds the duration of the whole transmission and ACK phase.

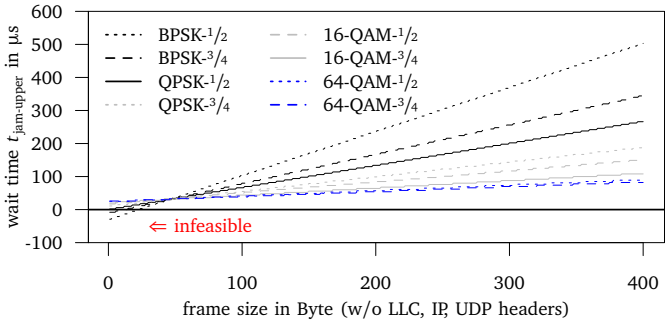


Figure 2. Jamming unicast ACKs for different payload sizes and data rates.

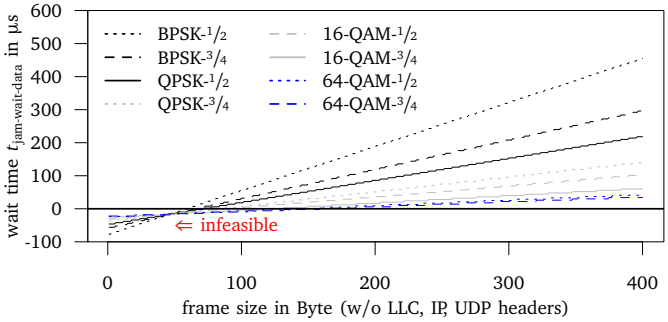


Figure 3. Jamming DATA frames for different payload sizes and data rates.

In Figure 2, we see that for almost all configurations it is possible to jam unicast ACKs. Only for very robust MCSs and small frame sizes the delay $T_{\text{jam-delay}}(N_{\text{DBPS}})$ is too large to transmit an interference frame in time.

Similarly, we can derive the waiting time to not jam the ACK but the unicast frame as

$$t_{\text{jam-wait-data}} = t_{\text{tx}}(L_{\text{DATA}}) - T_{\text{jam-delay}}(N_{\text{DBPS}}), \quad (3)$$

for which we show in Figure 3 the results for different MCSs and payload sizes.

To interfere very small data frames is more challenging in terms of timing constraints since the additional times t_{SIFS} and $t_{\text{tx}}(L_{\text{ACK}})$ cannot be taken into account. Still, for larger frame sizes and higher MCSs the data frames still can be jammed.

IV. CONCLUSION

In this paper, we study the feasibility of jamming WLAN data frames and, as a novel aspect, control frames such as unicast ACKs with commodity WLAN hardware. We also provide an analytical analysis of timing calculations to allow precise calculation of when to transmit an interference frame. Our results show that we are able to jam WLAN ACKs for almost all unicast frame length configurations.

REFERENCES

[1] T. X. Brown, J. E. James, and A. Sethi, "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks," in *ACM MobiHoc 2006*, Florence, Italy: ACM, May 2006.

[2] M. Vanhoef and F. Piessens, "Advanced Wi-Fi Attacks Using Commodity Hardware," in *ACSAC 2014*, New Orleans, LA: ACM, Dec. 2014, pp. 256–265.

[3] D. S. Berger, F. Gringoli, N. Facchi, I. Martinovic, and J. Schmitt, "Friendly Jamming on Access Points: Analysis and Real-World Measurements," *IEEE Transactions on Wireless Communications*, vol. 15, no. 9, pp. 6189–6202, Sep. 2016.

[4] M. Schulz, F. Gringoli, D. Steinmetzer, M. Koch, and M. Hollick, "Massive Reactive Smartphone-Based Jamming using Arbitrary Waveforms and Adaptive Power Control," in *ACM WiSec 2017*, Boston, MA: ACM, Jul. 2017, pp. 111–121.

[5] G. Chen and W. Dong, "JamCloak: Reactive Jamming Attack over Cross-Technology Communication Links," in *IEEE ICNP 2018*, Cambridge, UK: IEEE, Sep. 2018, pp. 34–43.

[6] F. Klingler, F. Dressler, and C. Sommer, "The Impact of Head of Line Blocking in Highly Dynamic WLANs," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7664–7676, Aug. 2018.

[7] B. Bloessl, F. Klingler, F. Missbrenner, and C. Sommer, "A Systematic Study on the Impact of Noise and OFDM Interference on IEEE 802.11p," in *IEEE VNC 2017*, Torino, Italy: IEEE, Nov. 2017, pp. 287–290.

[8] IEEE, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE, Std 802.11-2012, 2012.