Gaining Insight on Friendly Jamming in a Real-World IEEE 802.11 Network

Daniel S. Berger*, Francesco Gringoli†, Nicolò Facchi†,
Ivan Martinovic‡, and Jens Schmitt*
*DISCO Lab, University of Kaiserslautern, Germany
†CNIT - DII, University of Brescia, Italy
‡University of Oxford, United Kingdom
{berger,jschmitt}@cs.uni-kl.de,
{francesco.gringoli,nicolo.facchi}@ing.unibs.it,
ivan.martinovic@cs.ox.ac.uk

ABSTRACT

Frequency jamming is the fiercest attack tool to disrupt wireless communication and its malicious aspects have received much attention in the literature. Yet, several recent works propose to turn the table and employ so-called friendly jamming for the benefit of a wireless network. For example, recently proposed friendly jamming applications include hiding communication channels, injection attack defense, and access control.

This work investigates the practical viability of friendly jamming by applying it in a real-world network. To that end, we implemented a reactive and frame-selective jammer on a consumer grade IEEE 802.11 access point. Equipped with this, we conducted a three weeks real-world study on the jammer's performance and side-effects on legitimate traffic (the cost of jamming) in a university office environment. Our results provide detailed insights on crucial factors governing the trade-off between the effectiveness of friendly jamming (we evaluated up to 13 jammers) and its cost. In particular, we observed – what we call the power amplification phenomenon – an effect that aggravates the known hidden station problem when the number of jammers increases. However, we also find evidence that this effect can be alleviated by collaboration between jammers, which again enables effective and minimally invasive friendly jamming.

Categories and Subject Descriptors

C.2.1 [**Computer Communication Networks**]: Network Architecture and Design—*Wireless communication*

Keywords

friendly jamming; jamming for good; defensive jamming; reactive jamming; IEEE 802.11; Wi-Fi; WLAN

WiSec'14, July 23–25, 2014, Oxford, UK.

ACM 978-1-4503-2972-9/14/07 ...$15.00.
http://dx.doi.org/10.1145/2627393.2627403.

1. INTRODUCTION

Radio frequency jamming is commonly understood as a severe threat to the security and availability of wireless networks. Such intentional interference effectively disrupts communication on the physical layer making mitigation hard. In the military context, jamming is an established primitive to block an enemy's communication, and even practical handbooks on this topic are available [1–3, 25]. The same threat, however, also applies to the availability of civilian communication networks and received significant research interest (e.g., [21, 23, 24, 27, 38]). Seen from the attacker's perspective, jamming is a simple, yet effective tool. However, these are also desired properties for defense tools of a system and thus the question arises why not view jamming as a protection tool.

This question has recently motivated many researchers to envision positive use cases of jamming in wireless networks (cf. a list of proposals in Table 1). Such positive use cases, however, have different requirements on the jamming technique. In the traditional attack setting, the jammer attempts to block any communication usually only subject to stealthiness or energy constraints [23, 24]. On the other hand, realistic scenarios in which jamming is used to benefit network operations introduce an orthogonal requirement: *minimal invasiveness*. In particular, in order to coexist with other legitimate networks, only specific transmissions should be targeted, whereas the impact on other transmissions should be minimal. We henceforth denote by *friendly jamming* such use cases in which jamming is used for the good and strives to be minimally invasive.

While there are different jamming techniques (cf. a discussion in Section 2), minimal invasiveness requires reactive and frame-selective jamming. Reactive jamming has been characterized to be energy-efficient and effective [40], and is more likely to comply with legal regulations[1]. Actually applying friendly jamming in practice, however, faces many challenges. Reactive and frame-selective jamming poses strict timing constraints, and involves further engineering issues for which solutions have begun to emerge in recent years.

[1]For example, the maximum duty cycle (the fraction of one second a transmitter is active) is commonly limited to small values [10]. We briefly remark, however, that jamming, in general, is a sensitive topic. For example, in the US the operation, marketing, or selling of continuous jammers such as GPS jammers, or cell phone blockers is prohibited [11].

Related Work	Technology	Problem addressed	Js	Methodology
Jamming for good [22]	802.15.4	fake messages, unauth. comm.	3+	implementation and evaluation
WiFire [36]	802.15.4	unauthenticated comm.	2	implementation and evaluation
IMD shield [12]	(propriet.)	unauth. comm.,eavesdropping	1	implementation and evaluation
Jamming for Throughput [7]	802.11	performance: hidden terminals	1	theoretical analysis
Ally Friendly Jamming [31]	802.11	unauthenticated comm.	2+	analysis, implementation, and evaluation
Defend your home [6]	802.15.4	unauth. comm., fake messages	1	implementation and evaluation
Shout to Secure [16]	802.11	eavesdropping	1	simulation
iJam [13]	802.11	key generation	1	implementation
Secure Wi-Fi Zones [17]	802.11	eavesdropping	4+	theoretical analysis and implementation
Wire-Tap Channel	(indep.)	eavesdropping	1	theoretical analysis, implementations

Table 1: This study is concerned with scenarios requiring a *minimally invasive* and distributed jamming system (and an IEEE 802.11 b/g network). Similar scenarios are assumed in [6,7,12,22,31,36], whereas [13,16, 17] and also the Wire-Tap Channel scenario (umbrella term coined by Wyner [39], see also [8,20,30,33,41,42]) usually do not assume minimal invasiveness, e.g., the whole channel is often continuously blocked.

Hence, a critical issue is whether friendly jamming works as desired under *real-world* conditions, i.e., under multipath effects and attenuation, or fast channel fading in a dynamic environment. On a high level, this is thus the key question we address in this paper: *Is friendly jamming practically viable in a real-world 802.11 network?*

Answering this question by a real-world measurement study, we delve into the details of two issues, the performance of jamming and its related cost. As we will see these two have to be traded off against each other and the details of that trade-off depend on several factors that we investigate. We base our measurement study on the most widely deployed wireless communication standard, IEEE 802.11. To that end, we implemented a friendly jammer by modifying the microcode of the wireless chipset in a customer-grade access point, which has been certified to comply with legal regulations on power and spectral density requirements. Over a period of three weeks we ran a friendly jamming scenario, recorded all messages exchanged at different vantage points, and investigated the jammer's performance as well as negative side-effects on legitimate traffic. By this, we hope to provide an understanding of friendly jamming "in the wild" and thus foster further research in this promising and interesting domain[2].

Specifically, we collected the following main insights from our real-world study:

1. We found clear evidence that a large number of jammers is required to ensure high hit ratios.

2. The sequence of unjammed frames possesses a memoryless property – rendering predictions based on past observations inefficient, which makes their exploitation harder (which is good).

3. The cost of friendly jamming lies mainly in what we call the *power amplification effect*, which results in an aggravation of hidden station problems.

4. Collaboratively selecting the best jammers can boost the effectiveness of multiple jammers while minimizing the cost of jamming.

[2]We distribute a ready-to run version of our implementation on our project page `http://www.ing.unibs.it/~openfwwf/friendlyjammer/`. It also holds condensed result tables and samples of the measurement data – we ask for brief email inquiry to obtain the full source code and measurement data.

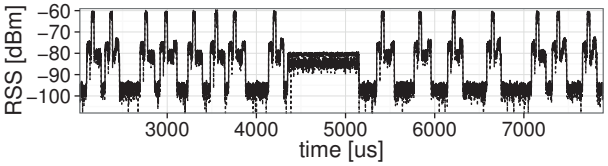

Figure 2: A particular challenge of friendly jamming is to enable coexistence with other legitimate networks' traffic (e.g., not to jam the beacon in the center) while accurately jamming target frames (here: all of the short frames).

5. In additional simulations based on our measurements we investigated more thorough the underlying reasons why perfect jamming is often infeasible.

The rest of this paper is structured as follows. In Section 2 we given an introduction to friendly jamming. The setup of our experiments is introduced in Section 3 and is followed by our main results in Section 4. Section 5 contains a technical analysis of jamming success. We discuss related work in Section 6 and conclude in Section 7.

2. FRIENDLY JAMMING: CONCEPTS AND CONSTRAINTS

There are several techniques to disrupt a wireless transmission. The most fundamental approach addresses the physical layer on which intentional interference causes errors when decoding a transmission's data. In this section we describe enabling techniques for (radio frequency) jamming; in particular, we focus on a description of reactive jamming as the technique, which lies at the foundation of friendly jamming. We conclude this section with an outlook on evaluation aspects for our real-world study.

2.1 Proactive vs. Reactive Jamming

There is a variety of techniques to create intentional interference. Continuously emitting a high power signal, for example, requires a lot of power and does not admit other uses of the channel. Other approaches are deceptive jamming (deceiving stations that the channel is occupied), random jamming (randomly alternating between sleeping and jamming), and reactive jamming [24, 40]. In reactive jamming, the interfering signal is emitted only when another signal is detected. This can be done selectively by analyzing

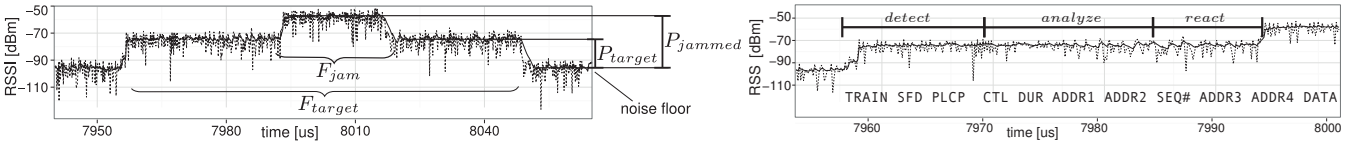

Figure 1: Left: in order for the jamming frame F_{jam} to successfully interfere with the target frame F_{target} (i.e., to render it irrecoverable) it is necessary that the superimposed signal's power P_{jammed} is significantly higher than P_{target}. Right: reactive jamming involves three steps: detecting the signal by means of the training sequence, analyzing the signal to decide whether or not to jam, and, if so, emitting the jamming signal.

signals and interfering only with certain ones. Therefore, reactive jamming is the most attractive jamming technique for friendly jamming and can yield minimally invasive applications. This technique is often considered the most sophisticated jamming technique [24] and entails several challenges.

2.2 Reactive Jamming Challenges

Reactive jamming starts with the task of channel sensing in order to detect a target frame (a signal in IEEE 802.11 terminology). The target frame's detection and further decoding can only be achieved by jammers which are well positioned with regard to the arriving signal (to be specific: the target signal arrives with high signal-to-noise-ratio (SNR)). This position, with respect to the sender and environmental conditions, is thus an important factor for jamming success.

After having detected the signal, the jammer starts the decoding and analysis in order to take a jamming decision. In a realistic scenario, the jammer needs to distinguish between target frames and legitimate frames (Figure 2). While the jamming hit ratio ($\#\,jammed\ frames\,/\,\#\,sent\ frames$) of the former needs to be maximized, the impact of jamming on the latter shall remain small. This trade-off is further constrained by the fact that the decision has to be taken very fast. We recall these timing constraints by considering, say, a frame comprising a medium-sized 100 Bytes UDP packet. If this frame is transmitted at the fastest 802.11g Modulation and Coding Scheme (MCS), its duration is only $48\mu s$. If we further assume that the jamming decision depends on bits in the MAC header (e.g., the sender's MAC address), the remaining part of the frame is even another $24\mu s$ shorter. In the remaining time, the jammer's decision code has to be executed, the hardware needs to switch from receive to transmission mode, and the jamming signal has to be emitted.

Once the signal is emitted, successful jamming depends on the target frame's MCS and the jamming signal's power. While higher power drives high jamming success, this factor is subject to legal regulations and is a crucial factor for the detrimental impact on legitimate traffic. A final aspect concerns the systems view of jamming as concurrent jammers can improve upon both the target frame detection and the jamming signal's power level. Therefore, the number of concurrent jammer is another important success factor.

2.3 Evaluating Friendly Jamming

In comparison to an attacker's perspective on jamming, friendly jamming demands a broader evaluation scope. While the jammer's hit ratio (and corresponding factors) are an important performance aspect, we additionally have to consider some friendly jamming specific aspects. In particular, estimating the cost of jamming in terms of potential negative side effects on other legitimate transmissions is of great interest. Another question poses itself for friendly jamming in a security setting: is an attacker on the network able to predict jamming misses (which could then be exploited)? This predictability constitutes the main attack vector on friendly jamming systems and, accordingly, should be kept as low as possible. Finally, we argue that an experimental friendly jamming deployment has to be considered from a worst-case perspective. Therefore, our experimental setup assumes a random placement of jammers instead of choosing preoptimized jammer positions.

3. EXPERIMENTAL SETUP

A practical evaluation of the factors described in the previous section requires a realistic implementation and evaluations in a complex radio communication environment. In this section we briefly introduce our realization of a friendly jammer, some micro benchmarks to ensure the system's basic operation, and the deployment used for the result in Section 4.

3.1 Jammer Hardware and Implementation

In order to encounter realistic hardware constraints, we implemented the reactive jammer for our experiments on cheap customer-grade hardware that has been certified to comply with regulatory rules. We start with a brief description of this jammer.

Our jammer is implemented directly on the Network Interface Card (NIC) of the popular WRT54GL platform. Access to this resource was facilitated by an open source microcode for the access point's IEEE 802.11 NIC (released by the OpenFWWF [14] project). This microcode replaces the proprietary Broadcom image and allows direct control of all medium access, decoding, and encoding operations subject to some (humble) hardware constraints due to the microcontroller's original purpose. Similarly to [5, 28] we altered the receive path in the assembly code and compiled the jammer's functionality in our own microcode that would be run directly on the NIC.

A principal advantage of the Broadcom NIC that we used is that the microcode can analyze a frame while still receiving it: this feature enables us to implement flexible filtering rules to decide whether or not to emit a jam signal. For example, the check can be based on matching an incoming frame's header to a dynamic bit mask dynamically configured from the host system. The experiments in Section 4, however, are based on a simple match of a frame's transmitter address. After the jamming decision has been positively evaluated, the jammer aborts the current reception, switches to transmission mode, and delivers the jam frame to a serializer, which further handles its emission through the RF circuitry. The jam signal has to be a standard compliant

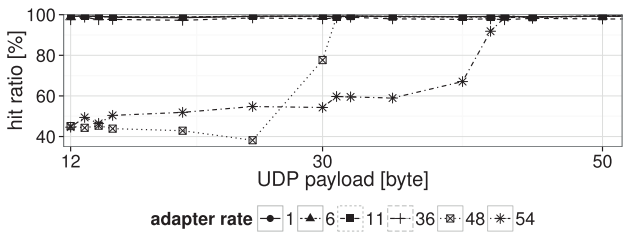

Figure 3: Impact of F_{target}'s duration: short frames at high rate cannot be jammed, e.g., at $54Mb/s$ frames with less than 42 bytes payload.

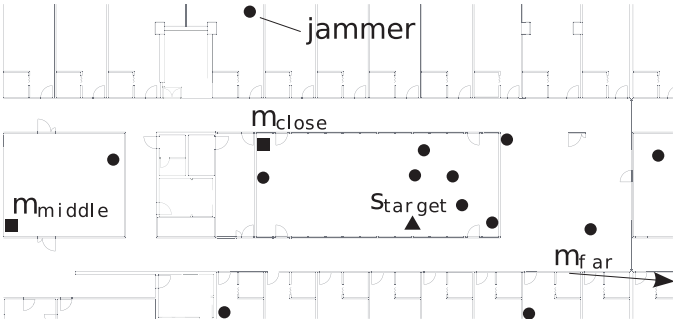

Figure 4: The target traffic source (s_{target}) and 13 jammers were located in a $30m \times 45m$ segment of the floor. The monitored experiment area is in total $40 \times 85m$ (extends to the right), and covered by m_{close}, m_{middle}, and m_{far}, which is located far to the right.

frame, but can be assembled directly on the NIC and is only constrained by the hardware's capabilities[3].

The fact that the WRT54GL is based on particularly cheap Broadcom NIC had (besides some challenges) also advantageous side-effects: due to some randomness in execution timing and significant clock skew, multiple jammers behave independently which results in a higher likelihood to cause destructive interference (cf. Section 5).

3.2 Micro Benchmarks and Optimal Jamming Signal

Several micro benchmarks validated the sanity of the jammer implementation. For example, traces by real-time spectrum analyzers (Figure 2) showed that target frames were jammed reliably and accurately, while legitimate traffic remained unjammed.

As a consequence of these micro benchmarks, we implemented several code optimizations to shorten the jammer's reaction time and increase jamming performance. For example, the jammer's configuration was originally stored in a part of the NIC's memory that can be accessed from the host system and the microcontroller to enable flexible reconfiguration. However, as this access is slow, we implemented a prefetching mechanism that stored the jammer's configuration in fast-access registers. Another optimization addressed the chipset's sending power management, which is based on partial information from reverse engineering the chipset. We ran comprehensive tests on corresponding hardware registers before settling on a final configuration.

We also found that the jamming frame's MCS impacts the jamming performance. We fixed it to the best configuration, which was attained by $1Mb/s$ DSSS jamming signals. For this MCS, the impact of the jamming frame's payload length was negligible and the MAC Protocol Data Unit (MPDU) was set to ten bytes (the minimal length allowed by the hardware). The jamming signal then $192\mu s$ for the transmission of the Physical Layer Convergence Protocol header, and additional $80\mu s$ for the MPDU – a total of $272\mu s$ in air time.

We also obtained the reaction time of the jammer as the time it took to react after matching a specific MAC address. By comparing original and jammed frames' content, we verify this delay to be two bytes at $1Mb/s$, i.e., $16\mu s$. Independently, the minimal frame length that can be jammed verifies this finding as Figure 3 shows that the jammer implementation can tackle frames with at least 42 bytes at 54 Mbps or 31 bytes at 48 Mbps.

3.3 Deployment and Device Configuration

We selected a university office floor as a representative and challenging setting since it is a particularly heterogeneous and dynamic environment. The university network's traffic is generated by a dynamic user base of faculty members and students; it comprises a variety of traffic sources such as typical back-office activities, research oriented applications, and even multimedia applications. Besides the university's main campus network, there are various smaller access points with many overlapping Basic Service Sets, so that we are able to observe different networks types in parallel.

We deployed 13 WRT54GL wireless access points as jammers, four additional WRT54GLs configured as two sources-sink pairs, and three Alix2d2 system boards as monitors on the university floor. The target traffic source was located at a fixed position, s_{target} in Figure 4. It generated an iperf UDP stream at a constant rate that was sent to a corresponding sink at a short distance. We experimented with different traffic rates, inter-frame spacing (e.g., SIFS) and backoff mechanisms but finally chose a standard-compliant configuration at a low rate of $500Kb/s$ in order to allow legitimate traffic to be observed on the same (and adjacent) channels.

Our measurements are taken by additional traffic monitors, which were placed at three observation points. These locations were constrained by availability, and are shown in Figure 4: in the same room (m_{close}), in an adjacent room (m_{middle}), and in a large office room down the floor (m_{far}) (also see Figure 11). Another source-sink pair was placed in the same room (not shown in Figure 4) and injected additional artificial crosstraffic to measure application-level performance of regular users with ongoing jamming.

We took particular care to preserve the association of s_{target} to its access point by filtering out deauthentication messages: this was necessary as the controller of the University wireless network was reacting to our experiment setup using the same channels by sending spoofed deauthentication messages. By eliminating unintended causes of lost F_{target} we were able to reliably generate traffic that we transmitted using a round-robin rate selection without retransmissions, in order to obtain uniform statistics for each

[3]To be specific the jammer can use DSSS and ERP-OFDM, but neither HT nor VHT, and only in the $2.4GHz$ band

dist	1 Jammer	2 Jammers	3 Jammers
5.4m	98.93% (±0.19)	100.0% (±0.00)	99.98% (±0.02)
6.7m	98.57% (±0.85)	99.95% (±0.04)	100.0% (±0.01)
8.1m	77.03% (±12.30)	98.37% (±0.29)	99.43% (±0.14)

Table 2: Open-space hit ratio (97.5% confidence intervals) under $1-4$ jammers and different distances.

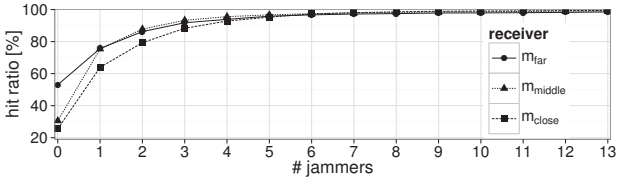

Figure 5: The hit ratio is significantly lower in-doors than in open-space due to attenuation. (0 jammers corresponds to packet loss without jamming.)

MCS. To accurately track sent, received, and valid-checksum statistics, we implemented corresponding low-level counters that were not impacted by the operation system.

In summary, our setup was carefully crafted to obtain reliable target traffic and accurate measurements.

3.4 Measurement Data

The experiments were conducted over a three week period In November and December 2013 to observe different conditions and utilization of the wireless channel. Time was divided into short experiments each of about 150s, where in each experiment a random number and selection of jammers were activated uniformly from all possible combinations. In total, this setup generated 13660 experiments with about 350GB of measurement data comprising almost 370 million target frames and 490 million legitimate-traffic frames.

This concludes our description of the experimental setup and we next report on the insights obtained in this setting.

4. RESULTS ON FRIENDLY JAMMING IN THE REAL WORLD

In this section, we investigate the trade-off between jamming performance and the cost of friendly jamming under (worst case) random selection of jammer positions; while the jamming performance increases with the number of jammers, the cost of jamming also goes up. We also find evidence that friendly jamming can overcome the constraints of this trade-off by collaboration schemes that heuristically select the most appropriate subset of jammers.

The confidence intervals throughout this section give 97.5% confidence based on the t-distribution. We start by describing performance aspects of friendly jamming under the factors discussed in Section 2.

4.1 The Jamming Performance

A direct metric to determine a jammer's performance is the hit ratio for which Figures 5 and 6 show a selection of significant factors.

Number of Jammers. We first evaluate the effect of the number of jammers being used. Both in an ideal open-space environment (Table 2) and our dynamic indoor setting (Figure 5), an increasing number of jammers increases the hit ratio due to improving the detection and emitted power of

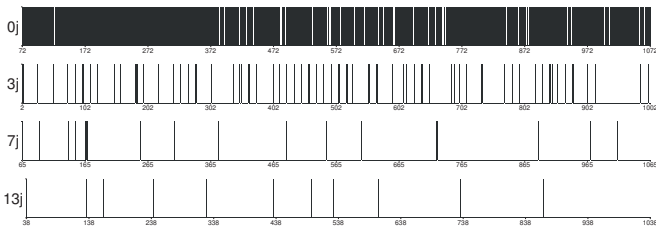

Figure 7: Sequence number diagrams visualize the requirement for several concurrent jammers. From above to below: 0, 3, 7, 13 jammers. In each, black bar: valid checksum, white bar: jammed.

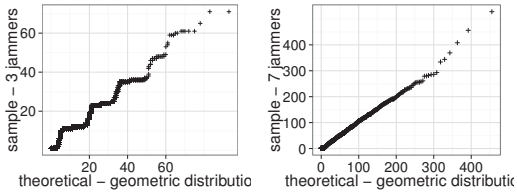

Figure 8: Quantile-quantile plots show good correspondence with a geometric distribution for seven jammers (right) but not for three jammers (left).

the jammers. Note, however, that in the open-space environment one may grossly underestimate the number of jammers necessary for the realistic environment. We observed that a single jammer significantly impacts the target packet rate. Nevertheless, some positions close to the target receiver yield low hit ratios – an observation that can be partly explained by the high and irregular attenuation of the office environment (also see the analysis in Section 5). Due to this, a single jammer's hit ratio lies between $60-90\%$ (averaged over all positions). At least three jammers are required to sustain an average hit ratio above 90%, seven jammers for 99%, and the hit ratio graph's slope only flattens out for more than eleven jammers. This appears to be robust across receivers at different proximities, which yielded distinct packets loss rates without any jammers ($19-48\%$ at $12-75m$, cf. Figure 4). These figures are probably higher than expected and must be taken as caveat for friendly jamming applications.

Position-Dependence. In a open-space testbed the hit ratio monotonically decreases with the jammer's distance from the receiver; in contrast to this, in-door behavior is quite erratic and there are weak positions even close to a target receiver (cf. Figure 6(left)). The impact of these weak positions is more pronounced for robust MCSs (those which are based on direct sequence spread spectrum), and lower numbers of jammers. For example, the hit ratio when averaging over random placement of three jammers decreases significantly for the robust MCS $1Mb/s$, as shown in Figure 6(center). Already for seven jammers, this issue mostly disappears as it is more likely that a good position is included in the active jammer set.

Invariance to Seasonal Effects. Figure 6(right) shows the average rate of legitimate traffic and the hit ratio of three and seven jammers over the measurement period. While the legitimate traffic rate shows the expected habitual variations, the hit ratio remains pretty stable for both three and seven jammers. For three jammers, we observe some exceptions to this, e.g., on November 20 the hit ratio of three

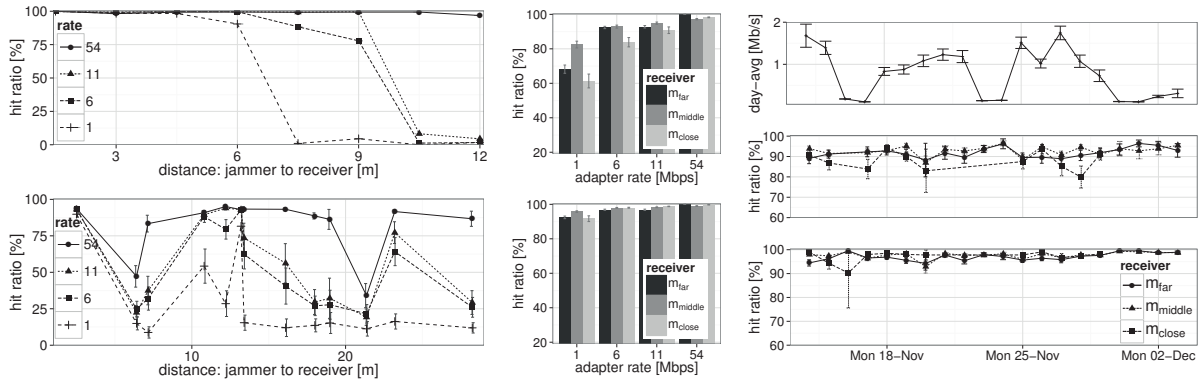

Figure 6: Left: in open space a single jammer's hit ratio decreases monotonically with the distance (top), whereas the indoor evaluation shows erratic behavior (bottom), indicating the need for careful real-world deployments. Center: robust adapter rates (MCSs) such as 1Mb/s have a tremendous impact on the hit ratio of three jammers (top), but less on seven jammers (bottom). Right: while the legitimate traffic's throughput shows weekly patterns (top), the hit ratio of three (center) and seven (bottom) jammers remain almost stable.

jammers goes down significantly due to some untraceable events about which we could only speculate. Note, however, that we observe no impact on seven jammers.

Temporal Distribution of Misses. Besides the hit ratio, another metric to determine a jammer's performance can be based on temporal correlations of missed frames. If jamming is used to block an attacker from sending, e.g., malicious packets, then runs of consecutively missed frames constitute a greater threat compared to the case in which the same number of frames was missed spread-out over time. Figure 7 shows a sequence number diagram of representative traces, which depicts how increasing the number of jammers yields a more uniform distribution of the missed frames over the sequence number space. We formalize this aspect by a stochastic miss model. The quantile-quantile plots in Figure 8 show that for seven jammers, the geometric distribution yields a good fit. Since the geometric distribution is memoryless, i.e., having observed any number of past misses does not yield information about a future miss, this property ensures that the prediction of future target frame misses (attack opportunities) is hard – even when an attacker is able to observe the friendly jamming system over a long time. However, our analysis shows that at least seven jammers are required to provide this property. For example, three active jammers are not enough to enforce this property (Figure 8(left)).

This section gave an overview on global jamming performance aspects. Note that the specific values of the hit ratio depend on our implementation, which we deliberately based on cheap customer-grade hardware as a feasibility study. However, we argue that some of the fundamental properties presented in this section apply to a much broader set of jammers, which adhere to FCC or EU regulations.

The next section focuses on an orthogonal aspect – how invasive is friendly jamming.

4.2 The Cost of Friendly Jamming

In this section, we investigate the side effects of friendly jamming on *legitimate* traffic in the network. Note that legitimate frames have not been targeted by the frame-selective jammers; instead, any adverse effect on legitimate traffic is collateral – the cost of friendly jamming.

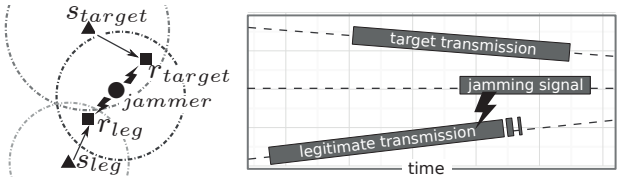

Figure 9: Assume that a target transmission and a remote legitimate transmission would be interference free without jammer. Nevertheless, a jammer located between them may interfere with both transmissions: intentionally, with the target transmission; collaterally, with the legitimate transmission. We call this effect power amplification.

In order to assess this cost, we distinguish legitimate frames from target frames (and, possibly, jamming signals) in our measurement data. This required some attention because fragments resulting from the target and jammers' frames could not easily be distinguished from actual legitimate frames due to high bit error levels. We used a two-run procedure on the measurement data: the first run discovered valid legitimate transmitter MAC addresses, and the actual analysis was carried out on a second run in which frames with small Hamming distance from the legitimate addresses were considered. This analysis was also verified selectively down to the bit level of individual frames.

Loss of Legitimate Traffic and Power Amplification. Increasing the number of jammers affects legitimate differently depending on their respective positions (with regard to the target sender and the jammers). We attribute this effect to what we call the power amplification effect: the jammers can significantly increase the interference radius of any target transmission. This can be seen by considering a scenario (see Figure 9 for an illustration) in which a legitimate sender is located far away from the target sender and transmissions of the two senders would be free of interference. Assume a jammer is located between the two senders and can receive and interfere with transmissions of both senders. If the legitimate sender starts a transmission, the target source could possibly start a concurrent transmission as well. Without jammers, both transmissions may proceed without prob-

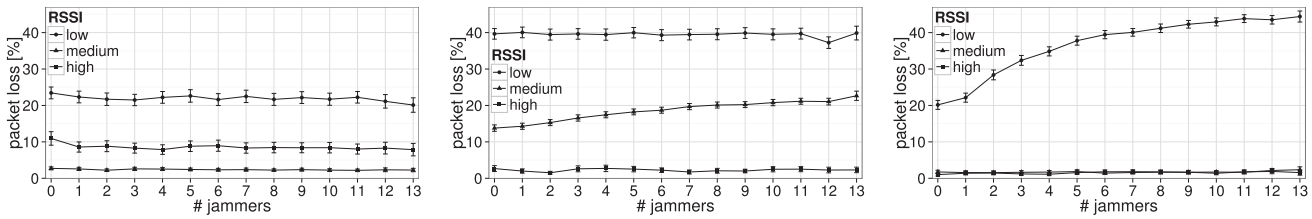

Figure 10: Packet loss of legitimate traffic characterized by respective RSSI levels. Left: the data from monitor m_{close} shows stable behavior. Center: monitor m_{medium} observed an increase in the packet loss for senders with medium RSSI, which we attribute to a slight power amplification effect. Right: the packet loss of traffic from low RSSI senders to m_{far} doubles with an increasing jammer count.

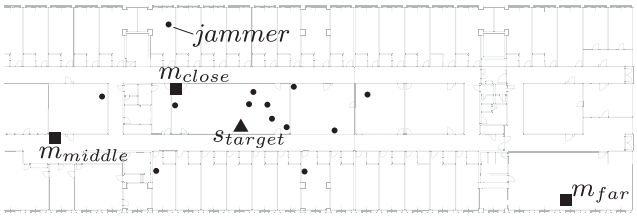

Figure 11: Monitored experimental environment.

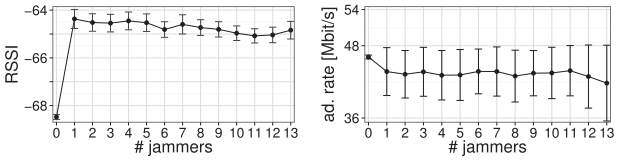

Figure 12: Left: the RSSI (at m_{close}) surges when enabling the first jammer, indicating an increased noise level. Right: the mean adapter rate of artificial traffic slightly decreases with the # of jammers.

lems; once the jammer selectively interferes with the target transmission, however, it also creates interference with the legitimate transmission, causing it thus to fail.

We quantify this effect by exploiting the fact that our monitors m_{close}, m_{middle}, and m_{far} cover a large observation area, 85m in length (see map in Figure 11). For each of the monitors, we categorize the observed senders into three classes based on the received signal strength: low RSSI ($< -65dB$), medium RSSI ($-65dB <$ RSSI $< -55dB$), and high RSSI ($> -55dB$). The packet loss for each sender in these classes is measured with the monitor as a receiver, based on each frame's checksum. Figure 10 reveals that the packet loss increases with the number of jammers only for two classes (and is stable for the other classes). The most badly affected class is the traffic with low RSSI as observed by m_{far} (Figure 10(right)): the packet loss doubles from 20.2% to 40.4%. The low-RSSI senders are located at positions to the right on the floor (Figure 11), where they do not receive the target messages but may suffer interference from the jammers in the center (i.e. the setting described in Figure 9). Accordingly, we attribute the observed increase of packet loss to the power amplification phenomenon, for which the likelihood increases with an increasing number of active jammers. The second affected class are m_{middle}'s medium-RSSI senders (Figure 10(center)): the packet loss increases from 13.7% to 22.6%. We also explain this observation with the jammer's power amplification; however, the effect is less pronounced than before since there are fewer candidate jammers. It is also interesting to note that the low-RSSI senders at m_{middle} are not similarly affected by this phenomenon – we attribute this to erratic propagation effects of the indoor topology (cf. Figure 6(left)); for example, there is a fire door to the left of this monitor that significantly alters signal propagation paths.

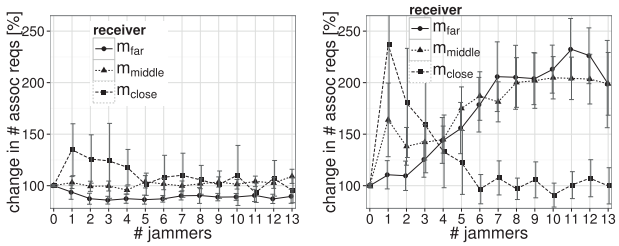

Figure 13: On average, the number of (re)association requests remains approximately stable (left). However, some particular stations are badly affected (right: most badly affected station).

Summing up, we found that friendly jamming can substantially impair the channel of legitimate transmissions due to the power amplification effect. Future studies of friendly jamming should thus seriously consider a cost perspective besides traditional metrics of performance and security.

Interaction with Rate Adaptation. The remaining station's packet loss is only marginally affected by higher jammer counts. Curiously, we find that the close-by traffic's loss (Figure 10(left)) slightly decreases when the first jammer is enabled. This is probably due to the close-by stations' rate adaptation algorithms. When considering the RSSI recorded at the close-by monitor, we find that it increases significantly (Figure 12(left)). From this we infer a generally increased level of channel noise, which triggers the rate adaption algorithms to select a more robust modulation. In fact, Figure 12(right) shows that the mean adapter rate shows more variance when the jammers are enabled and slightly tends towards more robust MCSs. The effect on the mean adapter rate of packets at different monitors is even smaller.

Effect on Associations. As a final aspect of the cost of jamming, we consider the number of (re)associations requests under different numbers of jammers. Figure 13(left) presents the change in this number with respect to the configurations without jammers. While the close-by stations seem to be affected by an increase of up to 40%, the farther-away stations exhibit approximately stable behavior. We also considered

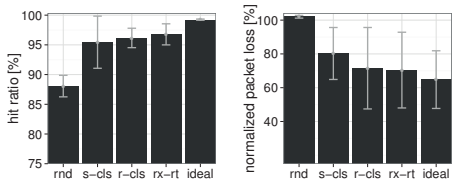

Figure 14: Left: the hit ratio of the proposed jammer-collaboration schemes. Right: the packet loss of far-away packets (affected by the power amplification phenomenon) normalized to random jammer configurations with the same hit ratio.

the (re)associations of individual stations, and found that there is a small number of significantly affected stations. Figure 13(right) depicts that there exist some far-away stations that loose connectivity more likely with an increasing number of active jammers. Interestingly, we also found evidence of a close-by station, which is more badly affected when there is a small jammer count.

In summary, we again emphasize the trade-off between jamming performance and the cost of jamming: enabling a larger number of jammers is necessary to boost the hit ratio but also increases the collateral damage to legitimate traffic. While not unexpected, we obtained detailed quantitative statements on the cost of jamming in a real-world 802.11 network. These results were obtained under the assumption of random jammer placement – a limitation a jamming system might be able to overcome, and which we investigate in the following section.

4.3 Jammer Collaboration Schemes

In this section, we show the potential of jammer collaboration, by which we mean that jammers are selected according to some deterministic rule instead of randomly as above. This promises to improve the hit ratio while remaining marginally invasive, based on the previous section's finding that the jammer's position is critical to both the performance and cost of friendly jamming. We investigate this potential by comparing three practical collaboration schemes to the theoretic optimum observed in our experiments.

The simplest idea is to select the jammer closest to the sender (e.g., realized by trilateration) and is called *s-cls*. If the jamming system can observe bidirectional communication attempts between targets, the jammers may be able to infer the location of the intended receiver and the jammers closest to the receiver can be selected. One can expect the corresponding scheme, *r-cls*, to improve the hit ratio because respective jammers would be closer to the receiver and thus their jam signals arrive with higher energy. Our third practical scheme is based on the idea to select jammers based on their reception quality. More specifically, the scheme *rx-rt* selects those jammers that received the highest number of target frames. While this heuristic only considers the channel from the receiver to the jammer, one may speculate that it also corresponds to better jamming positions in general.

We evaluate these schemes' performance with three jammers. The theoretical *ideal* scheme, which always picks the most successful jammers based on a posteriori knowledge, and the average performance of random jammer placement are considered as ground truth. Figure 14 compares the hit ratio of the schemes and the magnitude of their respective

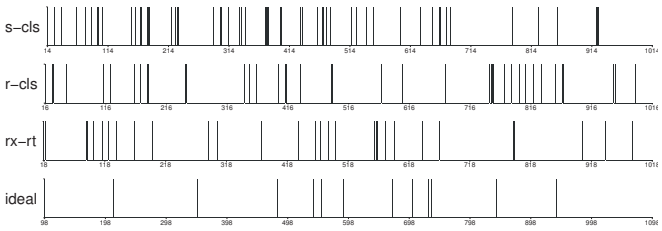

Figure 15: Sequence number diagrams shows the effectiveness of the collaboration schemes already for three jammers – compare to Figure 7.

power amplification effects. The latter is measured as the normalized packet loss of far-away packets where normalization is done to configurations that yield the same hit ratio[4].

The simple *s-cls* scheme significantly increases the jamming performance and also reduces the effect of the power amplification phenomenon. We attribute this improvement to the fact that the receiver and the sender are positioned close to each other and far-away jammers are efficiently excluded. The extension, the *r-cls* scheme, yields a slightly better hit ratio than *s-cls* and can reduce the packet loss even further. However, we remark that this scheme is less practical than *s-cls*. The third practical scheme *rx-rt* can outperform *s-cls* slightly, but with overlapping confidence intervals. While all collaboration schemes improve significantly over random jammer selection, their hit ratios are $2.5-4\%$ below the *ideal* case – indicating some further room for improvement and more sophisticated schemes.

We also compared sequence number diagrams of the four proposed collaboration schemes. Figure 15 displays the differences of the schemes with respect to this performance metric. It again also shows the gap in performance to the *ideal* case. Nevertheless, while the misses of the random jammer selection do not possess the memoryless property of the geometric distribution, the misses of all collaboration schemes come closer (*r-cls*) or achieve it (*s-cls*, *rx-rt*).

We also studied the schemes for seven jammers. In that case, the mean hit ratio is about 98.95% for *s-cls*, 99.41% for *r-cls*, 99.62% for *rx-rt*, and 99.95% for the *ideal* case.

This completes the measurement analysis, and we next address the jamming success in more detail.

5. DETAILED ANALYSIS OF JAMMING SUCCESS

In the previous section, we observed friendly jamming to hit target traffic only imperfectly as there will always be some successfully received frames under power constraints. This finding holds even under very favorable conditions: the long-term hit ratio in a static environment (at night) with large numbers of jammers with constant jamming power never reaches 100%. Under the assumption that only detection, reaction time, and power determine jamming success (for fixed MCS and other conditions), one may wonder why this is the case. This section investigates explanations for this somewhat mysterious finding. In particular, we also address the reason why jamming affects frame differently despite equal power levels.

[4]If scheme x achieves a hit ratio of 90%, the normalized packet loss of x is: (packet loss of x) / (packet loss of random jammer configuration, which yields a 90% hit ratio)

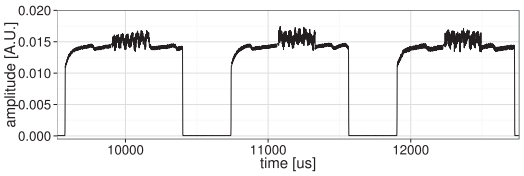

Figure 16: Three jammed frames in a Tektronix trace. The first frame is jammed and yields a wrong checksum with our software decoder, while the following two frames can be decoded correctly (despite the same relation of P_{jammed} to P_{target}).

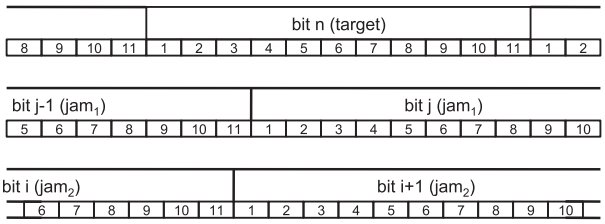

Figure 17: Alignment of two jam frames with a target frame: although none of the two jam frames is bit aligned, the top one achieves maximal, the bottom one minimal jamming success.

5.1 The Reception Process of DSSS

As expected and validated by our measurement results, the MCS underlying the 1 Mb/s rate is particularly robust to jamming and can be considered the worst-case with respect to jamming success. Thus, we focus our study on the corresponding direct sequence spread spectrum (DSSS) scheme and first review the reception process as defined in the IEEE 802.11 standard [15].

In the encoding process, bit are first pre-processed to be balanced, i.e., to not include long runs of binary 0s or 1s, and have a self-synchronizing property (→scrambling). Then, the DSSS scheme expands every bit into eleven chips that are mapped to a Barker sequence making it robust (→spreading gain). The Barker chips are then modulated with (differential binary) phase-shift keying (PSK) modulation, and the resulting symbols are transmitted.

Decoding starts with the receiver detecting energy on the channel. It then starts a phase-locked loop and the PSK can be demodulated to obtain the sequence of Barker chips. With the scrambled bit's self-synchronizing property, the actual data bits can finally be obtained.

In order to reliably decode a frame, the receiver has to synchronize with the incoming transmission. For instance, the border of each eleven Barker chips corresponding to one data bit have to be found. This is accomplished at the start of a frame by the physical layer preamble, which comprises a training sequence of 128 1-bits. Because the training sequence is known, the receiver can align its decoding components with the incoming data. The end of this sequence is indicated by the start of frame delimiter (SFD) (cf. Figure 1) and the receiver goes on to decode the remainder of the frame. Therefore, the alignment of the decoder with the frame remains robust despite interference and the spreading gain (the eleven-fold redundancy) can be used to recover the original bit sequence.

5.2 Impact of a Jammer's Symbol Alignment

At a receiver antenna, the two streams of symbols produced by the target and the jammer will not likely align, for several reasons: first, the clocks of jammer and target are not synchronized; second, the propagation delays could be different and change at every transmission because of multipath effects; third, the microcontroller of the jammer, its execution pipeline state and the instruction that is being executed when the target frame is received, strongly influences the scheduling delay of the jam signal. All these reasons are independent, and we assume in the following that the symbols in a jam frame can have any alignment with respect to those in the target frame and that the symbol delay can be approximated by a uniformly distributed random variable over an interval of symbol length. On a higher order temporal scale, there is also an issue with bit alignment: however, as we will show in the following subsection, it is symbol alignment to really make a difference and, in fact, there is only one possible symbol alignment scheme that minimizes jamming performance, i.e., when each jam symbol spreads over two consecutive target symbols (which in Fig. 17 happens for the bottom jam). On the contrary, there are eleven possible bit alignments that behave in the same way, which correspond to the number of symbols (or chips for $1Mb/s$) that compose each bit.

5.3 Trace-based Simulation Results

We developed the software-equivalent of an IEEE 802.11 receiver in order to simulatively validate the symbol alignment explanation as a root cause for unsuccessful jamming. The following simulation results are based on an actual trace of I/Q samples recorded with a real-time spectrum analyzer (Textronix RSA3408) during the real world experiments. Our spectrum analyzer captures traces with 12 bit resolution at $51.2MS/s$ which we downsampled to $44MS/s$ leading to four samples per Barker chip.

We validated our receiver on multiple traces of frames in which acknowledgments were clearly visible. The receiver works reliably and actually outperforms the hardware receivers used in the experiments. We also reproduced the previous finding, that different frames, which were jammed but agreed on the ratio P_{jammed}/P_{target} (cf. Figure 1), are sometimes successfully decoded but sometimes not. Figure 16 shows such an example in which the amplitude of three jammed frames looks similar, but only one in three can be decoded successfully.

Our first simulation of the symbol alignment addresses a valid capture of a single frame. We superpose this frame with another valid 802.11 $1Mb/s$ frame (the jam frame) at different symbol alignments and increasing amplitude (100% means same amplitude as the target). Given that we have four samples per symbol we can consider alignments in 25%-of-a-symbol steps. Figure 18(top) shows that for a fixed jam amplitude, the jamming success depends on the symbol alignment in a periodic fashion. If the jam amplitude is very low, all frames can be decoded; if it increases, jamming is successful at first in those cases in which the two frames are symbol aligned; if the amplitude is further increased, only those cases can be decoded in which the jamming frame is delayed by about 50% of a symbol. Finally, for high amplitudes, jamming is successful independently of the symbol alignment. We also evaluate for larger delays up to two

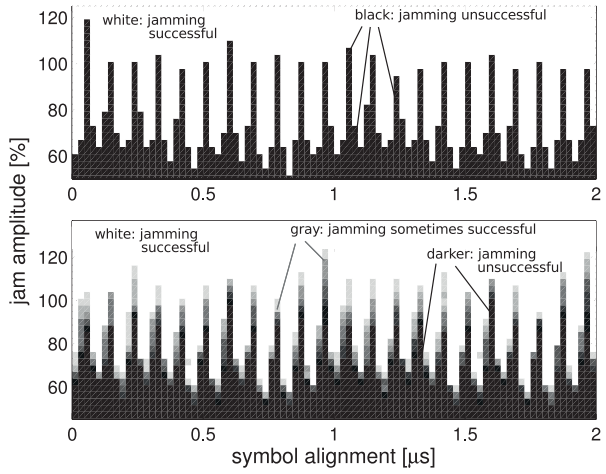

Figure 18: An explanation for the observation that jamming is only sometimes successful at the same jamming power: the jamming success depends on *both* the relative amplitude (jamming signal to target signal) *and* the symbol alignment. For each symbol, four alignments are displayed: jamming is successful for exact bit alignment (0%) and small deviation (25%, 75%). Jammed packets are often decodable for an alignment corresponding to a 50% symbol delay (the peaks). Top: single frame, bottom: entire trace with shades of gray corresponding to jamming/decoding probability.

full Barker chip sequences ($2\mu s$, 22 chips), but find that the jamming success is determined mostly by the alignment with respect to each symbol.

We next extend the same analysis to additional 27 frames. We can interpret this analysis stochastically as the probability that frames can be decoded for a specific combination of alignment and jam amplitude. Figure 18(bottom) shows that, in principle, the findings obtained for a single frame carry over to the other frames in our trace. However, note that there are subtle differences. For example, the minimal jam amplitude required increases by $3-5\%$ and the parameter regions indicating jamming success are less clearly defined. At the highest evaluated jamming amplitude of 120%, some frames can still be decoded for a particular configuration that corresponds to an alignment close to a full Barker sequence (close but not exactly bit alignment).

We also extended the simulations to the case of two jammers: the same method as before is used, but the jam frame is superimposed twice (independently) with all 28 frames in the capture. We explored the space of all possible symbol-alignments for both jam frames and consider the fraction of decodable packets for an equal amplitude for both jam signals. Figure 20 shows the improvement of a two-jammer configuration over a single jammer for low relative jam amplitudes of 37%, 59%, or 74% (from left to right). While most frames can be decoded for a single jammer, two jammers improve the jamming success rate significantly. Nevertheless, the actual effectiveness still depends on the respective symbol alignments: the jammers are successful if their alignment corresponds to delays close to 50%, as expected.

Finally, we connect the pieces of symbol alignment, jam amplitude, and the number of jammers: we consider the hit ratio as the average probability resulting under the assumption that any symbol alignment can occur with the same probability. Figure 19 shows that doubling the number of jammers more than doubles the hit ratio; for example, when the amplitude is 50%, a single jammer's hit ratio is maximally 20%, but with two jammers a hit ratio of $40-90\%$ can be obtained. This is due to the fact that unfavorable symbol alignments for several jammers at the same time become increasingly unlikely since the jammers behave independently (a probabilistic explanation results from the superposition of uniform distributions which result in low probability for simultaneously bad alignments).

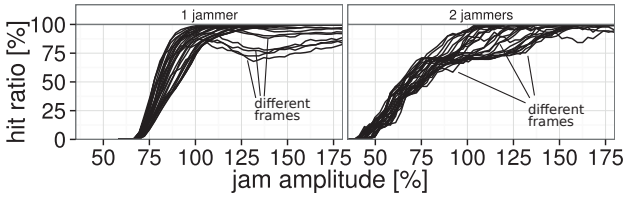

Figure 19: The simulated hit ratio for different frames (averaged over all symbol alignments) shows that two jammers significantly increase the hit ratio for low to medium jam amplitudes.

6. RELATED WORK

Friendly jamming relates to a variety of research topics in the field of radio communication. In this section, we briefly review previous work on friendly jamming applications, evaluations, and studies on interference properties.

Friendly Jamming Applications. Recent proposals can be roughly grouped into two main categories based on their intentions: 1) jamming for blocking unauthorized communications [6, 12, 22, 31, 36], and 2) jamming for improving secrecy of communications [12, 16, 17, 33] (see also works on the Wire-Tap Channel due to Wyner [39]).The first category is the most relevant motivation our study. For example, Gollakota *et al.* [12] and Brown *et al.* [6] propose to use reactive jamming to block unauthorized commands from being transmitted to implantable medical devices (IMDs) or to devices in the smart home. Similarly, Wilhelm *et al.* [36] rely on reactive jamming to enforce rules similar to a firewall. All friendly jamming proposals of this category share the goal of jamming only particular frames in the air motivating thus the evaluation of the cost of jamming in Section 4.2.

The second category also employs jamming as a tool but addresses a different use case. Intentional interference ensures that eavesdropping is rendered infeasible since the jammed messages cannot be decoded. Authorized nodes, however, can successfully receive the messages as the interfering signal is known to them (as a shared secret): these nodes cancel out the interfering signal to recover the original message. An interesting work by Kim *et al.* [17] defines a computational model to optimize the arrangement of jammers protecting an area around an access point. Their setting differs from our setting in that the jammers continuously emit a jam signal and the corresponding negative impact on other networks can only be controlled by power settings and the use of directional antennas (and is not evaluated in their work).

Evaluation of Friendly Jamming. Previous works mainly implemented reactive jamming on software defined radio (SDR) platforms (e.g., [4,6,36,37]) and did not target realis-

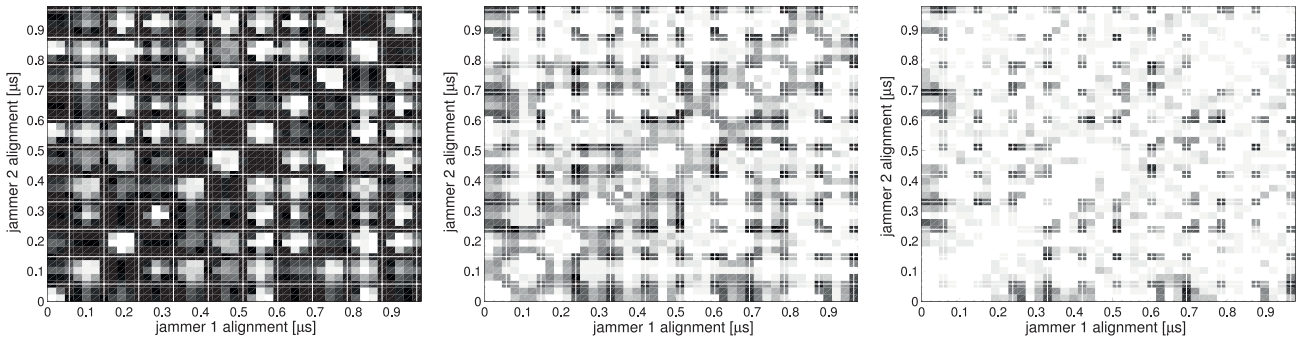

Figure 20: Results from simulations of two artificial jam frames indicate that the jam amplitude for successful jamming is significantly lowered, compared to a single jammer: while a relative amplitude of 37% (left) is ineffective, already 59% (center) greatly improves the jamming performance, for 74% (right) the jammers are almost always successful. These plots result from averaging over (all possible) alignments for 28 packets of a real trace (brighter shades of gray indicate higher jamming success).

tic customer-grade access points. The reaction times constitutes a particular challenge in enabling frame-selective jamming on these platforms. For example, Bayraktaroglu *et al.* [4] reports reaction times in the order of milliseconds and cannot target high-rate IEEE 802.11. Instead, the slower IEEE 802.15.4 standard has often been used to evaluate friendly jamming proposals. For example, Brown *et al.* [6] report hit ratios of $98.9 - 100\%$ in a testbed scenario and Wilhelm *et al.* [36, 37] achieve a reaction time of 39μs and a 97.6% hit ratio with one jammer (99.9 for two concurrent jammers) in an indoor office environment (however, for a short term, non-dynamic experiment).

To the best of our knowledge, we are the first to systematically evaluate the performance and cost of friendly jamming in a real-world environment. Having said that, the feasibility of friendly jamming with respect to secrecy applications, however, has recently been thoroughly evaluated by Tippenhauer *et al.* [32]. Their study focuses on a specific aspect compared to our more macroscopic view of friendly jamming: the confidentiality that can be provided by a jammer (see e.g., [8,12,20,30,31,33,41,42]). In their setting, the jammer and target source are located very close to each other ($15-30cm$) and communicate using the $400MHz$ band. For an attacker that is up to $3m$ away, Tippenhauer *et al.* demonstrated that jamming does not provide strong confidentiality guarantees for all configurations.

Interference and Collisions in 802.11. Our simulation study of jamming success is related to the study of packet error probabilities in face of non-intentional interference in IEEE 802.11 networks. These studies are largely motivated by the capture effect. The capture effect describes the successful reception of the stronger signal under interference (even if starting a little later) [18]. Although intentional inference motivates a different perspective (such as the one in Section 5), the corresponding analysis often tries to answer the same questions. In particular, while initial models only considered the role of relative timing on the frame level and the received power [18, 19, 34], more recent capture models report observations that agrees with our analysis.

These works come to a similar conclusion to ours, i.e., that the power ratio between interfering signals is not sufficient to build a capture effect model, but other parameters, such as time and phase offset of sender and receiver, have to be incorporated into the analysis [9, 19, 26, 29, 35].

7. CONCLUSION

System proposals for friendly jamming applications have received substantial research interest in recent years. Yet, a reality test was lacking, which is why we investigated friendly jamming at work in a real-word 802.11 network for three weeks. The main insights we collected from these are: 1) a rather high number of jammers is required to achieve a high hit ratio across different modulations, 2) the identification and quantification of the power amplification phenomenon which represents a shadow cost of friendly jamming, and 3) the effectiveness of potential jammer collaboration schemes in achieving a good trade-off between jamming performance and cost. The actual implementation of such collaboration is left for further study as it is most likely very application-dependent which scheme is realizable protocol-wise and which performance/cost trade-off needs to achieved. Besides the rather black-box oriented measurement results on friendly jamming, we also used simulations of the reception process of superimposed signals to investigate the question why perfect jamming is not always feasible. The analysis revealed a strong dependence of the jamming success on the symbol alignment between target and jam frame(s), opening up another interesting opportunity for future research: can friendly jammers boost their hit ratios by sending jam signals that are synchronized with the target signal? Throughout the paper, we assumed jammers to have no energy restrictions, yet, in the literature there are also jammers with a limited energy budget, therefore releasing this assumption could be another future work item.

Acknowledgments

We thank our anonymous reviewers for their insightful comments on improving various aspects of this work. In particular, we thank our shepherd, Panos Papadimitratos, for his valuable time and guidance. This research was partially supported by the EU's 7FP grant n.258301 (CREW).

8. REFERENCES

[1] D. Adamy. *EW 101: a first course in electronic warfare*, volume 1. Artech House, 2000.

[2] D. Adamy. *EW 102: a second course in electronic warfare*, volume 2. Artech House, 2004.

[3] D. Adamy. *EW 103: Tactical battlefield communications electronic warfare*. Artech House, 2008.

[4] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa. On the Performance of IEEE 802.11 under Jamming. In *Proceedings of IEEE INFOCOM*, pages 1265–1273. IEEE, Apr. 2008.

[5] G. Bianchi, P. Gallo, D. Garlisi, F. Giuliano, F. Gringoli, and I. Tinnirello. Maclets: Active mac protocols over hard-coded devices. In *Proceedings of ACM CoNEXT*. ACM, December 2012.

[6] J. Brown, I. E. Bagci, A. King, and U. Roedig. Defend your home!: Jamming unsolicited messages in the smart home. In *Proceedings of ACM HotWiSec*, pages 1–6, New York, NY, USA, 2013. ACM.

[7] Y. Cai, K. Xu, Y. Mo, B. Wang, and M. Zhou. Improving WLAN throughput via reactive jamming in the presence of hidden terminals. In *Proceedings of IEEE WCNC*, pages 1085–1090. IEEE, Apr. 2013.

[8] L. Dong, H. Yousefi'zadeh, and H. Jafarkhani. Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper. In *Proceedings of IEEE ICC*, pages 1–5, June 2011.

[9] P. Dutta, S. Dawson-Haggerty, Y. Chen, C.-J. M. Liang, and A. Terzis. Design and evaluation of a versatile and efficient receiver-initiated link layer for low-power wireless. In *Proceedings of ACM SenSys*, pages 1–14, New York, New York, USA, 2010. ACM.

[10] ETSI. EN 300 328 V1.8.1 Electromagnetic compatibility and Radio spectrum Matters (ERM), August 2012. `http://www.etsi.org/deliver/etsi_en/300300_300399/300328/01.08.01_60/en_300328v010801p.pdf`.

[11] FCC. Jamming Prohibition. last accessed 2014/13/02 `http://www.fcc.gov/encyclopedia/jammer-enforcement`.

[12] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu. They can hear your heartbeats: Non-invasive security for implantable medical devices. In *Proceedings of ACM SIGCOMM*, pages 2–13, New York, NY, USA, 2011.

[13] S. Gollakota and D. Katabi. Physical layer wireless security made fast and channel independent. *2011 Proceedings IEEE INFOCOM*, pages 1125–1133, Apr. 2011.

[14] F. Gringoli and L. Nava. Openfwwf: Open firmware for wifi networks. available at http://www.ing.unibs.it/ openfwwf/.

[15] IEEE. Standard 802.11 1999 edition (r2003) IEEE standard for information technology–telecommunications and information exchange between systems–local and metropolitan area networks–specific requirements–part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications, June 2003.

[16] M. Jorgensen, B. Yanakiev, G. Kirkelund, P. Popovski, H. Yomo, and T. Larsen. Shout to secure: Physical-layer wireless security with known interference. In *Proceedings of IEEE GLOBECOM*, pages 33–38, Nov 2007.

[17] Y. S. Kim, P. Tague, H. Lee, and H. Kim. Carving secure wi-fi zones with defensive jamming. In *Proceedings of ACM ASIACCS*, pages 53–54, New York, NY, USA, 2012. ACM.

[18] A. Kochut, A. Vasan, A. Shankar, and A. Agrawala. Sniffing out the correct physical layer capture model in 802.11b. In *Proceedings of IEEE ICNP*, pages 252–261, October 2004.

[19] J. Lee, W. Kim, S.-J. Lee, D. Jo, J. Ryu, T. Kwon, and Y. Choi. An experimental study on the capture effect in 802.11a networks. In *Proceedings of ACM WinTECH*, pages 19–26, New York, NY, USA, 2007. ACM.

[20] Z. Li, W. Xu, R. Miller, and W. Trappe. Securing wireless systems via lower layer enforcements. In *Proceedings of ACM WiSe*, pages 33–42, New York, NY, USA, 2006. ACM.

[21] G. Lin and G. Noubir. On link layer denial of service in data wireless LANs. *Wireless Communications and Mobile Computing*, 5(3):273–284, May 2005.

[22] I. Martinovic, P. Pichota, and J. B. Schmitt. Jamming for good. In *Proceedings of ACM WiSec*, page 161, New York, New York, USA, Mar. 2009. ACM Press.

[23] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou. A survey on jamming attacks and countermeasures in WSNs. *IEEE Communications Surveys & Tutorials*, 11(4):42–56, April 2009.

[24] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy. Denial of service attacks in wireless networks: The case of jammers. *IEEE Communications Surveys & Tutorials*, 13(2):245–257, 2011.

[25] R. Poisel. *Modern Communications Jamming: Principles and Techniques*. Artech House, 2011.

[26] C. Pöpper, N. Tippenhauer, B. Danev, and S. Capkun. Investigation of signal and message manipulations on the wireless channel. In V. Atluri and C. Diaz, editors, *Computer Security – ESORICS 2011*, volume 6879 of *Lecture Notes in Computer Science*, pages 40–59. Springer Berlin Heidelberg, 2011.

[27] D. R. Raymond and S. Midkiff. Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Computing*, 7(1):74–81, January 2008.

[28] P. Salvador, F. Gringoli, V. Mancuso, P. Serrano, A. Mannocci, and A. Banchs. Voipiggy: Implementation and evaluation of a mechanism to boost voice capacity in 802.11 wlans. In *Proceedings of IEEE INFOCOM*. IEEE, March 2012.

[29] N. Santhapuri, S. Nelakuditi, and R. Choudhury. On spatial reuse and capture in ad hoc networks. In *Proceedings of IEEE WCNC*, pages 1628–1633, March 2008.

[30] A. Sheikholeslami, D. Goeckel, H. Pishro-Nik, and D. Towsley. Physical layer security from inter-session interference in large wireless networks. In *Proceedings IEEE INFOCOM*, pages 1179–1187. IEEE, 2012.

[31] W. Shen, P. Ning, X. He, and H. Dai. Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time. In *Proceedings of IEEE S&P*, pages 174–188, May 2013.

[32] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun. On Limitations of Friendly Jamming for Confidentiality. In *Proceedings of IEEE S&P*, pages 160–173, May 2013.

[33] J. Vilela, P. Pinto, and J. Barros. Position-based jamming for enhanced wireless secrecy. *IEEE Transactions on Information Forensics and Security*, 6(3):616–627, Sept. 2011.

[34] K. Whitehouse, A. Woo, F. Jiang, J. Polastre, and D. Culler. Exploiting the capture effect for collision detection and recovery. In *Proceedings of IEEE EmNetS*, pages 45–52, May 2005.

[35] M. Wilhelm, V. Lenders, and J. B. Schmitt. An Analytical Model of Packet Collisions in IEEE 802.15.4 Wireless Networks. *CoRR*, abs/1309.4, 2013.

[36] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders. WiFire: a firewall for wireless networks. *Proceedings of ACM SIGCOMM*, pages 456–457, 2011.

[37] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders. Short paper: reactive jamming in wireless networks: how realistic is the threat? In *Proceedings of ACM WiSec*, pages 47–52, New York, NY, USA, 2011. ACM.

[38] A. Wood and J. Stankovic. Denial of service in sensor networks. *Computer*, 35(10):54–62, 2002.

[39] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, 1975.

[40] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of ACM MobiHoc*, pages 46–57, New York, NY, USA, 2005. ACM.

[41] X. Zhou and M. McKay. Physical layer security with artificial noise: Secrecy capacity and optimal power allocation. In *Proceedings of ICSPCS*, pages 1–5, Sept 2009.

[42] X. Zhou, M. Tao, and R. Kennedy. Cooperative jamming for secrecy in decentralized wireless networks. In *Proceedings of IEEE ICC*, pages 2339–2344, June 2012.