Lockpicking Physical Layer Key Exchange: Weak Adversary Models Invite the Thief

Daniel Steinmetzer
Secure Mobile Networking Lab
TU Darmstadt, Germany
dsteinmetzer@seemoo.tu-darmstadt.de

Matthias Schulz
Secure Mobile Networking Lab
TU Darmstadt, Germany
mschulz@seemoo.tu-darmstadt.de

Matthias Hollick
Secure Mobile Networking Lab
TU Darmstadt, Germany
mhollick@seemoo.tu-darmstadt.de

ABSTRACT

Physical layer security schemes for wireless communications are currently crossing the chasm from theory to practice. They promise information-theoretical security, for instance by guaranteeing the confidentiality of wireless transmissions. Examples include schemes utilizing artificial interference—that is 'jamming for good'—to enable secure physical layer key exchange or other security mechanisms. However, only little attention has been payed to adjusting the employed adversary models during this transition from theory to practice. Typical assumptions give the adversary antenna configurations and transceiver capabilities similar to all other nodes: single antenna eavesdroppers are the norm. We argue that these assumptions are perilous and 'invite the thief'. In this work, we evaluate the security of a representative practical physical layer security scheme, which employs artificial interference to secure physical layer key exchange. Departing from the standard single-antenna eavesdropper, we utilize a more realistic multi-antenna eavesdropper and propose a novel approach that detects artificial interferences. This facilitates a practical attack, effectively 'lockpicking' the key exchange by exploiting the diversity of the jammed signals. Using simulation and real-world software-defined radio (SDR) experimentation, we quantify the impact of increasingly strong adversaries. We show that our approach reduces the secrecy capacity of the scheme by up to 97% compared to single-antenna eavesdroppers. Our results demonstrate the risk unrealistic adversary models pose in current practical physical layer security schemes.

Categories and Subject Descriptors

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

Keywords

physical layer security; friendly jamming; artificial interference; key exchange; SDR; OFDM; WARP

WiSec'15, June 22 - 26, 2015, New York, NY, USA

DOI: http://dx.doi.org/10.1145/2766498.2766514.

1. INTRODUCTION

In recent years, novel and innovative physical layer security schemes have been put into practice in different application scenarios. Approaches based on artificial interference—also known as 'jamming for good'—have been widely discussed to enhance confidentiality in wireless communications. Apart from distorting wireless communications, jamming can be effectively applied to degrade the signal decoding at an eavesdropper. A closer look into current work reveals a number of shortcomings in practical solutions for physical layer security. In particular, we find attacker models to be severely constrained or unrealistic. In what follows, we present three defense schemes together with their main weaknesses.

Gollakota et al. apply jamming techniques to prevent unauthorized access to wirelessly accessible implantable medical devices (IMDs) that do not offer sufficient protection against attacks on their own. Their work [10] introduces an external shield to protect the devices by jamming the communication to potential attackers. Using such a shield prevents the inconvenient replacement of insufficiently protected IMDs by surgery. In [22], Tippenhauer et al. attack this scheme by placing the attackers' antennas equidistant to the jammer's antenna. This allows to suppress the jamming signal by destructive interference, while amplifying the used data signal.

In [3], Anand et al. aim at gaining confidentiality by transmitting a jamming signal together with the data signal. Using multi-antenna systems, the transmitter avoids jamming the intended receiver while disturbing any eavesdropper in its vicinity. Here, the sender uses a transmit filter that transmits artificial noise orthogonally to the intended receiver's wireless channel. To break this scheme, in [21], Schulz et al. assume a multi-antenna eavesdropper with capabilities similar to those of the sender in [3]. Additionally, they assume partial knowledge of the transmitted data to train an adaptive filter that spatially separates jamming from data signals. This paper highlights the need to evaluate physical layer schemes also employing existing attack methodologies, in this case transferred from the cryptography domain.

Another category of physical layer security schemes has been designed to perform key exchange in wireless systems. One practical example is iJam, introduced by Gollakota et al. in [11]. Here, jamming is used by the receiving communication partner to occasionally disturb a transmission of a secret key. Assuming that only the receiver knows which parts were jammed, an eavesdropper can neither suppress the jamming nor extract the exchanged key. The authors

assume a single-antenna eavesdropper. To the best of our knowledge, we are not aware of existing attacks against this scheme.

Summarizing, all of these physical layer security approaches use adversary models matching the capabilities of the defending systems. We argue that these adversary models are too weak for practical scenarios. The main problem is the assumption of only single antenna eavesdroppers.

In this work, we focus on the use of jamming detection mechanisms. Schemes like iJam rely on the fact that an eavesdropper should not be able to differentiate between jammed and naturally distorted signals. We demonstrate that the use of multiple antennas at the eavesdropper alone is sufficient to reliably detect the intentionally distorted information. Our contributions in this paper are the following:

- We introduce a new analysis scheme that distinguishes between jammed and unjammed transmissions based on the diversity of jammed signals.
- We apply our scheme on iJam [11], as a representative physical layer security scheme, and identify its benefits by utilizing multiple antennas.
- We implement our scheme in MATLAB for simulation and practical SDR-based evaluation with WARPLab using the wireless open-access research platform (WARP) [1].

Our results show that multi-antenna eavesdroppers (exploiting the signal diversity on different antennas) are able to mitigate the artificial interference caused by jamming signals. The capability to distinguish between jammed and non-jammed parts of a transmission gives multi-antenna eavesdroppers the ability to combine the correct signal parts containing the undisturbed key bits in iJam. We consider the action of breaking the key exchange scheme this way is comparable to 'picking a lock', which generally refers to opening a physical lock without the original key. With this, we practically outline the threat of multi-antenna eavesdroppers and show how easy attackers can improve their performance by using multiple antennas. In contrast to [22], we consider more than two eavesdropping antennas and do not assume them at specific locations. Our work aims at raising attention to the problem of refining realistic attacker models for future physical layer schemes.

This paper is structured as follows: in Section 2, we provide background information and related work on physical layer key exchange and artificial interference. In Section 3, we analyze the received signals and identify properties to distinguish clean and jammed signals. Based on our findings, we propose a concrete attack scenario and show under which circumstances eavesdropping becomes possible. Implementation details are provided in Section 4. We evaluate our findings in simulation and testbed experiments in Section 5 and show that a practical eavesdropper can obtain the secret key properly. Finally, we provide an outlook on future work conclude this paper in Section 6.

2. BACKGROUND AND RELATED WORK

In the following, we present related work in the area of physical layer security and describe how the key exchange scheme iJam works. Further, we discuss the commonly applied adversary model and outline the challenges for physical layer security schemes.

2.1 Physical Layer Security

Wireless communication systems are very important in today's society. However, due to the broadcast nature of wireless channels, attackers can easily eavesdrop on the communication. To defend against such attacks, confidentiality preserving techniques like encryption are required and generally employed from the data link layer upwards. The physical layer—where information is modulated into waveforms—is often ignored when it comes to securing communication systems. Regarding various attacks against cryptography or those bypassing cryptography, the physical layer offers an additional layer of protection. It uses properties based on signal propagation and wireless channel characteristics to increase the secrecy of a communication system.

The research interest into physical layer security in information theory is mainly driven by Wyner's idea of the wiretap channel [24]. Wyner shows that secrecy can be achieved on the physical layer as long as the eavesdroppers channel conditions are worse than those of the intended receivers. The challenge lies in designing protocols that degrade the eavesdropper's channel without disturbing the intended receiver.

A promising method to achieve this draws on friendly jamming—or 'jamming for good'—that blocks unwanted communication in wireless networks as described in [23]. Specifically applied to disturb eavesdroppers, the interference degrades the eavesdropper's reception without affecting the regular communication (see [8]).

The main purpose of *key extraction* and *key exchange* on the physical layer is to get keys for cryptographic algorithms operating on higher layers. Additionally, it is an example for the interaction between physical layer security and cryptography. *Key extraction* schemes, as presented in [16, 2], are based on the reciprocity of the wireless channel that allows to extract the same key on both ends. Several improvements accelerate the key generation rate using particular properties of the channel [25, 4, 7, 15, 17, 26]. The entropy of the extracted key mainly relies on the mobility of the devices or the environment. Hence, key extraction mechanisms exhibit low entropy and low key generation rates in static environments. They require extensive privacy amplification mechanisms to obtain keys with sufficient entropy [13]. *Key exchange* mechanisms as described in [11, 6, 19, 18], in contrast, do not rely on channel variations. They utilize physical layer mechanisms to confidentially transport existing keys to other communication partners without being eavesdropped. As this work focuses on the security of key exchange schemes, the following section deals with them in detail.

2.2 Exchanging keys on the physical layer

In *key exchange* mechanisms like iJam [11], two communication nodes agree on a shared key by partially jamming an exchange of random values. While one node transmits a random value, the other occasionally jams the transmission to prevent an eavesdropper from receiving. The iJam system model consists of three parties. We name them Alice, Bob, and Eve as depicted in Figure 1. Each of them is equipped with a single omni-directional antenna. It is Alice and Bob's intention to secretly exchange a key without Eve learning the key bits. The three parties behave as follows: Alice generates a random value and encodes it for wireless transmission but duplicates each symbol in the sig-

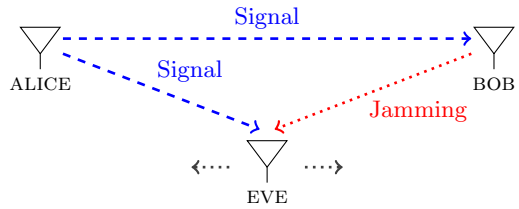


Figure 1: The key exchange system model: Alice transmits a signal to Bob, while Bob is jamming to distort Eve, who resides at arbitrary locations and observes the interference of both signals.

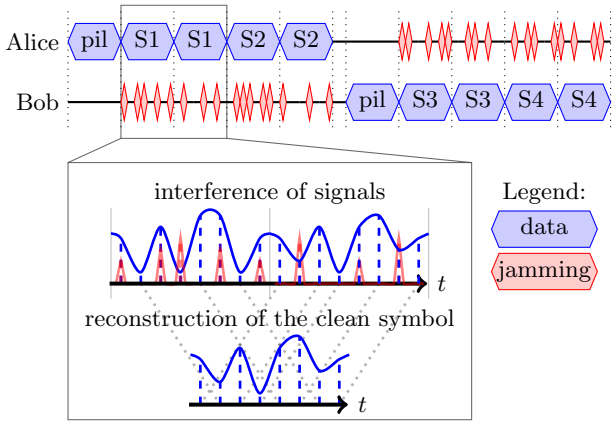


Figure 2: In iJam, Alice and Bob mutually exchange a secret while jamming. First, she transmits a signal with duplicated symbols and preceded pilot sequence while he is jamming. Afterwards, they switch roles and he transmits a signal while she is jamming. The jamming only distorts each signal part either in the first symbol or its repetition. To reconstruct the transmitted signal the unjammed parts need to be combined to a clean symbol.

nal. Each symbol, including the duplicate, is transmitted to Bob. At the time of reception, Bob transmits jamming signals at different powers that distort each sample; either in the original symbol or in the corresponding duplicate. Different powers are required to avoid jamming detections based on signal strength measurements at different positions around the communicating nodes. Since Bob knows which samples were jammed, he picks the clean samples and reconstructs the transmitted signal as shown in Figure 2. In contrast, Eve, who resides at an arbitrary location, is unable to distinguish between jammed and clean samples and, thus, is unable to decode the secret correctly. After Alice successfully transmitted a random value to Bob, both flip their roles and Bob transmits a random value to Alice in the same manner. Then, they compute the shared secret by concatenating the exchanged random values. The secret can then be used as a key to encrypt upcoming communications.

To guarantee the secrecy of the key during the exchange, iJam runs for multiple rounds. In each round, Alice selects a random value of fixed bit length and modulates it into an orthogonal frequency division multiplexing (OFDM) signal. Therefore, she maps the random bits to quadrature amplitude modulation (QAM) symbols that are distributed over the available OFDM subcarriers. Each of the generated OFDM symbols is duplicated before transmission and a pilot sequence is prepended. Bob uses the pilot sequence to detect the beginning of the transmission and starts jamming single samples of the signal. He either jams the original or the duplicated sample, and uses the respective other to reconstruct the complete information sent by Alice. Bob's jamming signal is Gaussian noise over the whole bandwidth used by the OFDM symbols.

When Alice transmits a time domain signal x_a and Bob jams with x_b, all nodes in vicinity receive a combination of these signals over different wireless channels. With h_a, we denote the channel impulse response from Alice, and with h_b the channel impulse response from Bob. Any node will receive the time-domain signal

$$y = h_a * x_a + h_b * x_b + n \tag{1}$$

where n denotes the noise present at the receiver. The symbol $*$ represents the convolution operation. To extract the information transmitted by Alice, Bob first needs to estimate the channel h_a using the pilot symbols transmitted by Alice. Then he uses the channel estimate to extract x_a. As Bob knows when his jamming signal x_b is zero, he knows which of the transmitted symbols are not disturbed by jamming.

2.3 Adversary model

Similar to most existing practical works, iJam considers a fairly simple adversary model. The adversary is a single passive eavesdropper that listens (with an omni-directional antenna) in wireless communications. She is able to move freely, but unable to be at multiple locations simultaneously. She can choose locations close to any communication party or reside directly in between them. Based on transmitted pilot sequences, the adversary is able to estimate the channels between herself and other communication parties. In general, the idea underlying iJam is that it is independent from the adversary's hardware. However, it assumes the adversary to utilize only one antenna and not to cooperate with other attackers. Neither multiple antennas nor directed antennas are considered.

Since eavesdroppers cannot be prevented from using multiple antennas, we extend our adversary model to multi-antenna eavesdroppers. On each antenna, the adversary receives superpositions of signals traversing different channels. In contrast to [22], she can freely choose her antenna locations. Even though we do not explicitly consider collaborative attackers, the principles we explain in the following can be adapted to them.

2.4 Design challenges in key exchange

To secure the key exchange, the system has to ensure that jammed samples are indistinguishable from clean samples and that jamming effects are independent from the adversary's location. In iJam, signals are OFDM modulated, which implies that signal samples are normally distributed in the time domain. The jamming impulses are also chosen from a normal distribution. Thus, also the superposition of both signals at the eavesdropper is normally distributed. Hence, jammed and clean OFDM signals look similar and are hard to distinguish.

According to [11], the effectiveness of jamming depends on the distances between Eve, Alice and Bob. Assuming Alice and Bob use the same transmit powers and Eve is close to

Bob, Eve receives Bob's jamming signal with higher power than Alice's signal. If Eve resides close to Alice, Eve is less affected by the jamming signal. To overcome the problem of simply choosing one location that is barely affected by jamming, iJam is performed mutually. Alice and Bob both take turns in sending and jamming. After Alice has transmitted a random value towards Bob, they switch roles, and Bob transmits, while Alice is jamming. To compute the shared secret, both transmissions are required. Hence, Eve cannot always reside closer to the sending or jamming party anymore. Gaining advantage in the first duration implies a disadvantage in the second duration and vice versa.

Eve aims at obtaining the transmitted key by listening in the transmitted data. She resides at an arbitrary location in the network but does not change it during protocol execution. She receives a combination of the useful and the jamming signal. However, unlike Alice and Bob, she lacks the information about jammed samples. She needs to compare two samples and decide for one to decode. Since both samples are normally distributed with zero mean, it is likely that samples with higher magnitudes are jammed. In [11], Eve distinguishes the samples based on their magnitudes according to a maximum likelihood hypothesis testing strategy:

$$|S_1|^2 \underset{H_2}{\overset{H_1}{\gtrless}} |S_2|^2 \tag{2}$$

where S_1 and S_2 are the received samples, H_1 denotes the hypothesis that S_1 is jammed, and H_2 the hypothesis that S_2 is jammed. However, the assumption that higher magnitudes indicate greater variances is quite unrealistic.

According to iJam [11], stated detection scheme, solely considering the samples' magnitudes, is the best guess the adversary is able to make. It is questionable if this is truly the best an adversary can achieve. Therefore, we consider a realistic and more powerful multi-antenna eavesdropper in this work and investigate if better attack results are achievable.

3. JAMMING MITIGATION

The previous section describes a physical layer key exchange scheme that proved to be effective in preventing single-antenna eavesdroppers from decoding a signal. Further questions arise as to whether multi-antenna receivers can improve decoding. In this section, we analyze how multiple antennas could exploit signal diversity to differentiate jammed and clean transmission.

3.1 Signal differences

To delve into the effects of multiple receiving antennas, we examine how jammed and clean signals differ from each other depending on the eavesdropper's location. Let Alice transmit a time-domain signal x_a, while Bob jams with x_b. Each of Eve's antennas receives a combination of both signals over different channels as shown in Equation 1. Regarding a single subcarrier k, we express the received signal on this carrier in the frequency domain as

$$X_{e_i}(k) = H_{a\to e_i}(k) \cdot X_a(k) + H_{b\to e_i}(k) \cdot X_b(k) + N_{e_i}(k) \tag{3}$$

where $X_a(k)$ and $X_b(k)$ are the Fourier transforms of x_a and x_b, $H_{a\to e_i}(k)$ and $H_{b\to e_i}(k)$ express the channel coefficients from Alice and Bob to Eve, and $N_{e_i}(k)$ denotes additional noise at Eve's ith antenna. Eve learns approximations to $H_{a\to e_i}(k)$ by estimating the channel coefficients with the prepended pilot sequences. However, since Bob does not transmit proper OFDM symbols when jamming, Eve is unable to learn $H_{b\to e_i}(k)$. Applying the channel correction by multiplying Equation 3 with the inverse of the estimate of $H_{a\to e_i}(k)$ results in the channel corrected signal

$$X_{e_i}(k) = \underbrace{X_a(k)}_{\text{signal}} + \underbrace{\frac{H_{b\to e_i}(k)}{H_{a\to e_i}(k)} \cdot X_b(k)}_{\text{interference}} + \underbrace{\frac{N_{e_i}(k)}{H_{a\to e_i}(k)}}_{\text{noise}} \tag{4}$$

which consists of the signal $X_a(k)$ plus interference of the jamming signal $X_b(k)$ and noise.

To evaluate the divergence of the received signal, let Eve compare the signals on two antennas $X_{e_1}(k)$ and $X_{e_2}(k)$. She computes the divergence as

$$\begin{aligned} \Delta X_e(k) &= X_{e_1}(k) - X_{e_2}(k) \\ &= \underbrace{\left(\frac{H_{b\to e_1}(k)}{H_{a\to e_1}(k)} - \frac{H_{b\to e_2}(k)}{H_{a\to e_1}(k)}\right) \cdot X_b(k)}_{\text{interference}} \\ &\quad + \underbrace{\frac{N_{e_1}(k)}{H_{a\to e_1}(k)} - \frac{N_{e_2}(k)}{H_{a\to e_2}(k)}}_{\text{noise}} \end{aligned} \tag{5}$$

that, under the assumption of perfect channel correction, consists of interference and noise only. In the jamming free transmission, the jamming part $X_b(k)$ remains zero and cancels out the interference. Thus, the divergence only depends on noise. If we assume that the noise in clean and jammed transmission has equal power, the divergence in jammed transmissions is higher than that observed in clean transmissions. Hence, we identify a property of physical layer signal propagation that indicates whether the signal has been jammed during transmission.

3.2 Exploiting signal diversity

Based on our findings on signal diversity on different receiving antennas (in particular higher divergence when jamming), we propose to exploit the diversity gain as an attack vector.

As stated above, Eve receives a combination of Alice's and Bob's transmitted signals x_a and x_b on each of her receiving antennas. While Bob knows which samples in the signal are jammed, Eve does not have this information. She needs to decide which of the two samples to decode. Since Eve's antennas are separated in space, they are affected independently by multi-path propagation. Alice's and Bob's signals overlap differently on each of Eve's antennas. In order to separate them, we come up with a detection scheme that does not require any knowledge on the channel towards Bob and aims to identify jammed samples in the signal.

To identify the jammed samples, Eve analyzes the impact of each samples on the frequency spectrum of the symbol. Let $s_{i,l}$, with $l \in [0, L-1]$, be the L time domain samples of an OFDM symbol received at Eve's ith antenna. To obtain the frequency domain of a signal, Eve typically applies a discrete Fourier transform (DFT). Since only individual samples are jammed, Eve needs to handle them individually. For each sample $s_{i,l}$, she computes the representative in the frequency domain by directly computing the frequency

Table 1: Summary of the major experimental goals and contributions of the paper

Experiment (technique)	Section	Results
Feasibility of lockpicking key exchange in noiseless environments (simulation)	5.3, 5.4, 5.5, 5.6, 5.8	Our multi-antenna approach enables Eve to reduce the secrecy capacity between Alice and Bob. Utilizing two antennas, the detection rate is as high as 84%.
Feasibility of lockpicking key exchange in different distances (simulation)	5.9	Our scheme has a low location dependency from a certain distance to Alice and Bob on. It performs best, if Eve is located equidistant to Alice and Bob.
Performance in a practical man-in-the-middle (MITM) scenario (testbed)	5.3, 5.4, 5.5, 5.6, 5.7	Our multi-antenna attack successfully eavesdrops on the key exchange. With four antennas, it reduces the secrecy capacity by 97.3%.
Feasibility of eavesdropping in vicinity (testbed)	5.9	Locations in very close proximity to any of the keying parties are unfavourable for eavesdropping on a mutual transmission.
Feasibility of lockpicking key exchange in a common office scenario (testbed)	5.11	Our eavesdropping attack suitably decreases the secrecy in non-optimal locations. Utilizing four antennas, we reduce the secrecy capacity by up to 84%.

components according to the DFT definition:

$$\mathcal{S}_{i,l}(k) = s_{i,l} e^{-j2\pi k \frac{l}{L}} \tag{6}$$

The resulting frequency domain value $\mathcal{S}_{i,l}(k)$ represents the information each sample $s_{i,l}$ provides to subcarrier $k \in [0, L-1]$. However, the frequency spectrum is still affected by channel distortions. To correct this, Eve multiplies $\mathcal{S}_{i,l}(k)$ with the corresponding inverse channel estimate in the frequency domain:

$$\tilde{\mathcal{S}}_{i,l}(k) = \mathcal{S}_{i,l}(k) \cdot H^{-1}_{a \to e_i}(k) \tag{7}$$

In a jamming and noise free transmission, this value should be equal on all antennas, since channel distortions are compensated. However, if the sample is jammed, artificial interference occurs and $\tilde{S}_{i,j}$ differs for a given sample j on each antenna i. Therefore, Eve computes a metric for sample l as variance of all corrected frequency spectra received with all antennas

$$m_l(k) = \mathrm{Var}\left[\tilde{\mathcal{S}}_{0,l}(k), \tilde{\mathcal{S}}_{1,l}(k), \ldots, \tilde{\mathcal{S}}_{I-1,l}(k)\right] \tag{8}$$

and takes the average over all subcarriers:

$$\overline{m}_l = \frac{1}{L} \sum_{k=0}^{L-1} m_l(k) \tag{9}$$

High values of $\overline{m}_l$ indicate high differences between the received samples on the antennas and, therefore, a high probability that the sample is jammed.

To apply the detection scheme, Eve waits until she receives a complete symbol with its duplicate. Then, she computes the metric given in Equation 9 for each sample in both symbols. Since each sample has been either jammed in the first or in the second symbol, she selects the symbol with lower $\overline{m}_l$. By appending all selected samples, Eve reconstructs the original symbols and decodes the transmitted signal by common means.

4. IMPLEMENTATION

We implement the physical layer key exchange mechanism and the multi-antenna eavesdropping attack in MATLAB while utilizing the WARP [1]. WARP is a SDR platform developed at Rice University. It provides great benefits for evaluation of communication systems on physical channels. For accessing WARP from MATLAB, we utilize the WARPLab framework. WARPLab allows to control and synchronize large arrays of WARP nodes from a single MATLAB instance.

Our signal modulation follows current WLAN standards. We use the 2.4 GHz band with 20 MHz bandwidth for transmitting signals. Since the WARP is operating at 40 MHz sampling rate, we need to upsample our signal. For symbol modulation of the source signal, we apply quadrature amplitude modulation (QAM). Each signal is composed of 64 subcarriers, of which 52 are used for data transmission. The OFDM symbol duration is 4.0 μs, from which 0.8 μs are needed for a cyclic prefix to mitigate inter-symbol interference (ISI). During one transmission we aggregate multiple OFDM symbols to one frame and prepend two pilot symbols. The jammer does not encode its signal as OFDM frames, instead, it transmits single random samples without prepending pilot symbols.

As transmissions and receptions in a WARPLab environment are only coarsely triggered by Ethernet frames, there can be offsets of multiple samples between the start of Alice's transmission and the start of Bob's jamming transmission and reception. The exact delay is found by cross-correlating the received frame preamble with a reference. Receivers compensates for it by shifting the received OFDM symbol by the estimated offset.

Since clocks on different WARP nodes slightly differ, the generated carrier frequency—used for up and downconversion of baseband signals—is set off. This effect, known as carrier frequency offset (CFO), has to be compensated for a successful reception. Our CFO estimator is based on the implementation presented in [20]. It estimates the CFO based on consecutive pilot symbols at the beginning of each frame.

5. EXPERIMENTAL EVALUATION

To illustrate the performance of our attack, we carry out simulations as well as practical measurements using the WARP. We evaluate different scenarios and use the secrecy capacity and jammed sample detection rate to describe the strength of the eavesdropper, Eve. In detail, we conduct five experiments, including two simulations and three practical testbed measurements. In each experiment we evaluate a different eavesdropping scenario. An overview of these experiments with evaluation goals and a summary of the achieved results is listed in Table 1. Our main goals are to outline the effects of jamming with different jamming gains, to demonstrate the feasibility of our detection scheme, and to expose the performance of this eavesdropping attack.

In all of our experiments, we vary the jamming gain as described in iJam [11] and consider Eve with a varying number of antennas. Using a single antenna only, Eve detects the jammed samples based on their magnitude. We consider this scheme our baseline as it was proposed as an attack in [11]. Using multiple antennas, Eve bases her decision on the divergence of the received signals at different antennas—the approach introduced in this work. We evaluate her performance with up to four antennas.

5.1 Evaluation setup

In each evaluation setup Alice transmits a random OFDM symbol to Bob while he transmits noise with varying power at the same time. Eve, receives a superposition of both signals on each of her four antennas. As she is not bound to a certain location, we move her around for different experiments. We repeat our experiments for each setting at least 200 times in our testbed experiments and 100 times in simulations.

To evaluate the optimal as well as the worst achievable eavesdropping performances, we assume that Eve knows which samples were jammed. We differentiate the optimal and worst case to obtain an upper and lower boundary on her performance. In the optimal case, Eve selects the unjammed samples and decodes the signal, like the intended receiver would do in a normal reception. The worst case portrays wrong filtering of the samples, which means that Eve selects the jammed samples for decoding.

In simulation, we perform experiments in MATLAB and use a channel model for indoor IEEE 802.11n wireless local area networks (WLANs) in office environments as proposed by Erceg et al. in [9]. In testbed measurements, we deploy WARP nodes for each communication party. To evaluate different jamming gains, we vary the transmission power of the jamming antenna in steps with size of 2 dB from 3 dB to 31 dB, while keeping the transmission gain constant at 15 dB. Figure 3 shows the setup for the MITM scenario with Eve located directly in between Alice and Bob with a distance of 1.20 m to each of them. In further experiments, we vary the location of Eve to assess her performance depending on her location.

Contrary to the simulation, we cannot receive and transmit signals concurrently in our testbed environment. The WARPLab framework only supports using each antenna either for transmission or reception. A full duplex signal processing chain is not provided. Hence, we need to focus our evaluation on the signals received at Eve and express the eavesdropping performance compared to what Eve could decode having jamming information. However, receiving the signal only at Eve does not prevent us from obtaining comprehensive results.

5.2 Evaluation metrics

In each iteration of the experiments, we transmit a sequence of random data and determine the bit error rates (BERs) at the receivers. Applying the model of the symmetric binary erasure channel [14], we determine the entropy of the received data as:

$$H(p) = -\left[p \cdot \log_2(p) + (1-p) \cdot \log_2(1-p)\right] \qquad (10)$$

where p is the probability for a flipped bit during the transmission that is the BER. The entropy expresses the receiver's uncertainty on the transmitted data. To measure the quality of a transmission, we use the channel capacity that is defined as $C = 1 - H(p) = 1 - H(\text{BER})$.

To measure the attack performance, we use the secrecy capacity C_s (as defined in [5]). Generally, C_s is defined as the channel capacity of the legitimate receiver, Bob, minus the capacity of the eavesdropper, Eve. In our setup, we redefine C_s to be the channel capacity C_{opt}—considering Eve having Bob's knowledge on which samples were jammed (optimal case)—minus the capacity C_{det}—Eve achieves by applying the presented jamming detection algorithm.

$$C_s = C_{\text{opt}} - C_{\text{det}} = H(\text{BER}_{\text{det}}) - H(\text{BER}_{\text{opt}}) \qquad (11)$$

A high secrecy capacity implies secure communication between Alice and Bob as well as low information leakage to Eve. To describe the performance of our eavesdropper, we compare the secrecy capacity achievable with a single eavesdropping antenna and that with multiple ones. The improvement is assessed as performance of our multi-antenna eavesdropping attack.

Along with the secrecy capacity, we evaluate the detection rate of jammed samples. The detection rate is the percentage of correctly detected jammed symbols and achieves values of 1.0 in the optimal case (detecting all clean samples correctly), and 0.0 in the worst case (detecting only jammed samples). An eavesdropper that randomly selects the samples for decoding achieves a detection rate of 0.5. To eavesdrop successfully, Eve needs to achieve a detection rate close to 1.0.

In the following experiments we evaluate all these parameters, namely channel capacity, secrecy capacity, and detection rate to demonstrate the performance of our eavesdropping attack.

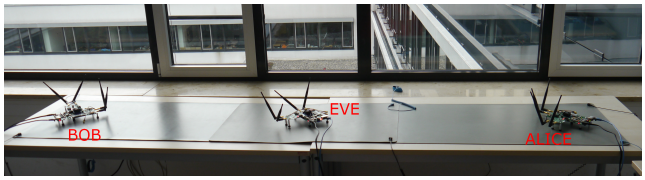


Figure 3: Experimental setup for the man-in-the-middle (MITM) scenario, showing WARP nodes for Alice, Bob, and Eve respectively.

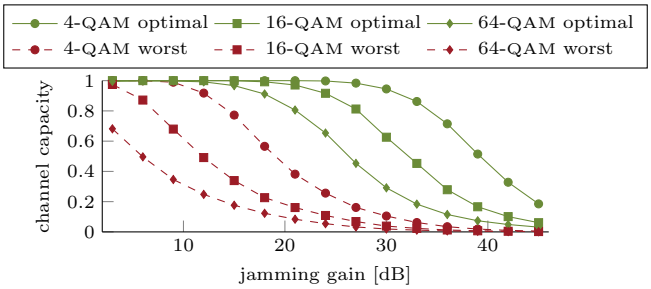


Figure 4: Channel capacity in noiseless simulation at the intended receiver in optimal and worst case.

5.3 The effects of different jamming gains

To express the effectiveness of the jamming signal, we regard the channel capacity in knowledge of the jamming information. The optimal reception that only selects clean samples for decoding should ideally approximate a channel capacity of 1.0 independent of the jamming gain. However, in our simulation of noiseless transmissions (depicted in Figure 4), we observe a decreasing channel capacity at Bob for high jamming gains, meaning that decoding errors occur. In practical measurements, in which Eve acts as man-in-the-middle (MITM), we observe the same effect (as illustrated in Figure 5), even though the measurements are not as pronounced as in simulation. Powerful jamming impulses still hamper clean samples. Transmitting a single jamming sam-

Table 2: Maximum achievable detection rates in simulation of a noiseless transmission and practical measurements in the MITM scenario

	simulation			measurements		
	4-QAM	16-QAM	64-QAM	4-QAM	16-QAM	64-QAM
1 ant.	0.5011	0.5013	0.5012	0.5016	0.5026	0.5030
2 ant.	0.8397	0.8398	0.8399	0.7982	0.8295	0.8451
3 ant.	0.8383	0.8386	0.8386	0.8529	0.8727	0.8883
4 ant.	0.8385	0.8389	0.8387	0.8805	0.8923	0.9033

ple results in several affected samples at the receiver. This leads to slightly increasing symbol errors for high jamming gains that decrease the channel capacity. With jamming gain, we refer to the antenna gain at the jamming node. The worst case illustrates the jamming effects. At low jamming gain, the jamming only causes marginal distortions that imply a high channel capacity. For increasing jamming gain, the channel capacity quickly decreases and approaches zero. Especially for medium jamming gains, the differences between optimal and worst case are obvious and represent the jamming efficiency.

5.4 The eavesdropper's channel quality

In contrast to the intended receiver (Alice or Bob), Eve lacks information about which samples were jammed by the receiver. Hence, she needs to extract clean samples using the jamming detection scheme presented in this paper. In Figure 6, we present Eve's channel capacities that we simulated for noiseless environments using one or two antennas. The channel capacities resemble those presented in Figure 4. Using only one antenna, the channel capacities approach the worst case performance at the intended receiver. Using multiple antennas, however, allows Eve to exploit the diversity of the received jamming signals. This way, she better resists jamming distortions and increases her channel capacity. Up to a jamming gain of 25 dB, only marginal channel degradations occur. Figure 7 shows the channel capacities in the MITM scenario, measured in our testbed. We observe that Eve's channel capacities approach the simulated optimal capacities very well, when using at least two antennas. Eavesdropping by using only one antenna, leads to channel capacities close to the simulated worst case.

5.5 The attacker's jamming detection rate

Up to this point, we concentrated on analyzing the channel capacity. However, this metric does not reveal how well the eavesdropper actually detects jamming. Hence, we introduce the detection rate that indicates how many jammed samples can be correctly detected by applying our jamming detection algorithm. We measure this rate as a percentage. Eavesdropping with a single antenna features detection rates around 0.5. Hence, the uncertainty if jamming occured or not is maximized. Using multiple antennas, however, increases the detection of correct bits to 0.84 in simulation.

In our testbed measurements of the MITM scenario, we observe similar results as in simulation (see Figure 8). In practice, the eavesdropper achieves detection rates of up to 0.83 with two antennas and 0.89 with four antennas. We list additional maximum detection rates in Table 2. We also observe that low jamming gains hinder the jamming detection the most and even multi-antenna eavesdroppers only

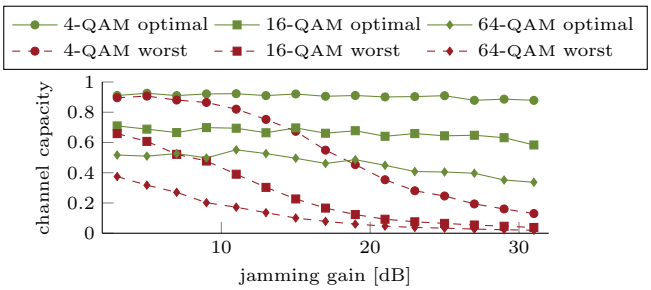


Figure 5: Optimal and worst case channel capacity at Eve in the MITM scenario (testbed) in knowledge of the jamming information

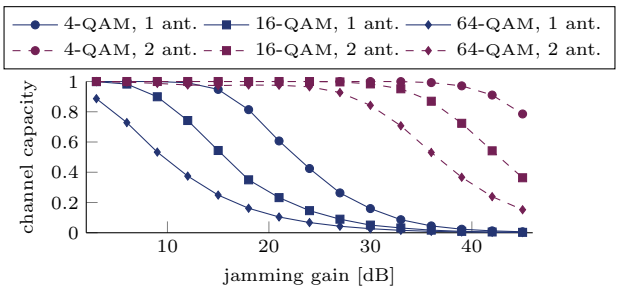


Figure 6: Channel capacity in simulation of noiseless transmission at Eve using either one or two eavesdropping antennas.

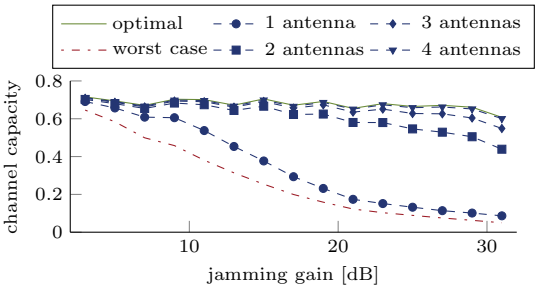


Figure 7: Channel capacity at Eve in the MITM scenario (testbed) when eavesdropping on 16-QAM modulated signals with optimal and worst case boundary.

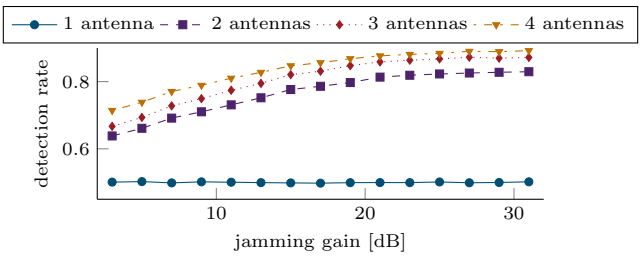


Figure 8: Detection rate in the MITM scenario (testbed) with 16-QAM modulated signals.

achieve moderate detection rates. This is due to small jamming signals that only cause small divergences on the receiving antennas making the detection algorithm falsely trigger on normal signal variations (e.g. due to noise). Considering that small distortions caused by small jamming signals only

have a small impact on the useful signal, it becomes superfluous to choose between the clean samples and the jammed ones when extracting the transmitted bits. This observation also reflects what we present in Figure 7, as low jamming gains still result in high channel capacities.

5.6 Secrecy capacities

The secrecy capacity represents the advantage of the intended receiver (in knowledge of the jamming information) over Eve who needs to detect jammed samples first. The simulated secrecy capacity for Eve using a single antenna as a function of the jamming gain for different modulation schemes is portrayed in Figure 9. Due to impairments in the channel quality for high jamming gains and negligible jamming effects for low jamming gains, it features a maximum at medium jamming gain. For low jamming gain, the jamming effects are simply too small to provide significant secrecy. For high jamming gains, the jamming causes interference with clean samples and thereby decreases the throughput between Alice and Bob, which also decreases the secrecy capacity. The average peak value of the secrecy capacity rise up to 0.76. In the practical experiment, we observe similar effects. The secrecy capacity in the MITM scenario using 16-QAM modulated signals, as shown in Figure 10, achieves a maximum 0.53 and therefore stays only slightly lower than that in simulation. If Eve uses multiple antennas for eavesdropping, the situation significantly changes. In simulation, two antennas are sufficient to reduce the secrecy capacity in 16-QAM and 4-QAM to zero. In 64-QAM, the secrecy capacity drops down to 0.016, and also disappears when using at least three eavesdropping antennas. In the MITM scenario, using two antennas instead of one reduces the secrecy capacity by 81.8% to 0.097. Using four eavesdropping antennas, the secrecy capacity drops down by 97.3% to 0.015. The maximum secrecy capacities for all modulation schemes are listed in Table 3. These results imply that, in contrast to a single-antenna eavesdropper, a multi-antenna eavesdropper breaks the security mechanisms of this physical layer key exchange.

5.7 Consequences of multiple antennas

While the number of receiving antennas affects the intended receivers performance only marginally, it significantly influences the performance of the eavesdropper. Using two eavesdropping antennas instead of only one, Eve massively increases her channel capacity. More antennas can further improve her results. With four antennas, Eve achieves an average channel capacity that approximates the optimal case very well. In simulation, Eve already reaches an optimal performance with two antennas. Practical measurements on our testbed are affected by noise, that multiple antennas can suppress. As shown in Figure 11, the detection rate increases in average by 64.1% with two, and by 77.6% with four eavesdropping antennas instead of one. The capacity decreases by 82.5% or 97.0%, respectively. These results show that Eve, in practice, is not as powerful as in simulation but compensates her impairments with extending number of eavesdropping antennas.

Table 3: Maximum achievable secrecy capacities in simulation of a noiseless transmission and practical measurements in the MITM scenario

	simulation			measurements		
	4-QAM	16-QAM	64-QAM	4-QAM	16-QAM	64-QAM
1 ant.	0.7853	0.7704	0.7500	0.5344	0.5340	0.3839
2 ant.	0.0000	0.0001	0.0163	0.0700	0.0970	0.0818
3 ant.	0.0000	0.0000	0.0000	0.0283	0.0391	0.0330
4 ant.	0.0000	0.0000	0.0000	0.0121	0.0146	0.0150

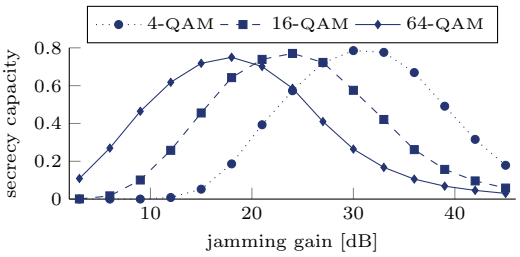


Figure 9: Secrecy capacity in noiseless simulation with Eve using a single antenna.

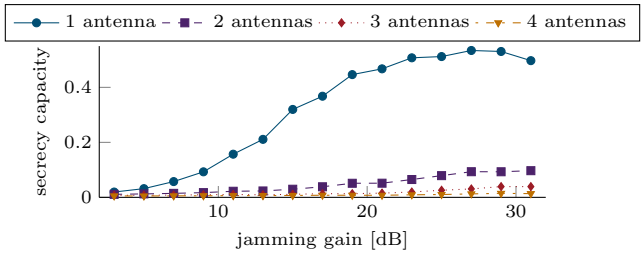


Figure 10: Secrecy capacity in the MITM scenario (testbed) with 16-QAM modulated signals.

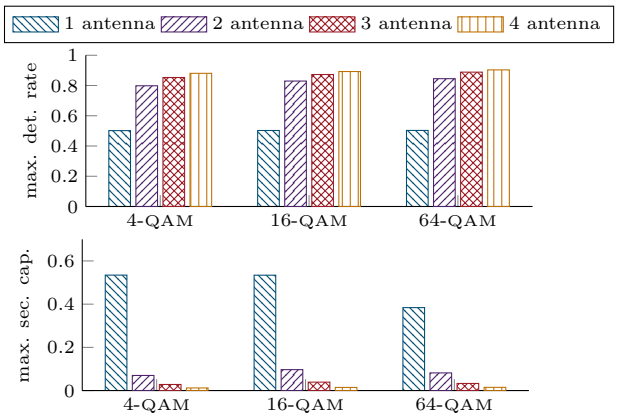


Figure 11: Maximum achievable detection rate and secrecy capacity in the MITM scenario (testbed) using different modulation schemes.

5.8 Impact of the modulation schemes

The effects of the jamming highly depend on the modulation scheme. Modulation schemes of high order exhibit a smaller Euclidean distance between the constellation points, which implies higher susceptibility for transmission errors and jamming. To successfully distort a symbol of low modulation order, a higher jamming power is required. Hence, the channel capacities in 64-QAM start decreasing earlier than in 16-QAM and 4-QAM. The behavior differs around 10 dB, as seen above. A similar observation can be made

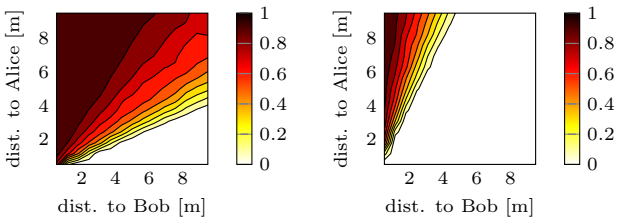
about the secrecy capacities. The maximum secrecy capacity is achieved at different jamming gains. Hence, changing the modulation index requires the jamming gain to be adjusted to achieve the same effects.

The maximum secrecy capacities and detection rates are independent of the modulation scheme. Only marginal differences are observable in simulation. Although different modulations require adjustments, the performance of our detection scheme remains independent from the modulation.

5.9 Dependency of the attacker's location

As seen in the previous evaluations, the performance of the physical layer security scheme highly depends on the jamming gain. In the second simulated experiment, we therefore evaluate different distances of Eve to Alice and Bob. We only consider one transmission direction in which Alice transmits while Bob is jamming. The other case can be estimated by flipping Eve's distances to Alice and Bob. Applying the model of free space path loss, we imply different received signal gains at Eve depending on her relative location to the keying parties. Doing so, we estimate the secrecy capacity by using a single antenna as shown in Figure 12a, and by using two antennas for eavesdropping as shown in Figure 12b. In the former case, we observe that the secrecy rate raises up to the maximum when Eve resides closer to Bob than to Alice. Hence, Eve is highly affected by jamming and cannot extract any information from the received signal. When Eve stays close to Alice, she observes the transmitted signal with highly attenuated jamming. Despite lacking jamming knowledge, she decreases the secrecy capacity close to zero. With equal distance to both of Alice and Bob, Eve achieves a similar secrecy capacity to that occurring in noiseless transmissions. This corresponds to the operation region of the iJam protocol as stated in [11]. When Eve utilizes two antennas for eavesdropping the secrecy region decreases massively. Regardless of her location, she performs better than by using a single antenna. With at least a certain distance to Bob, the secrecy capacity becomes close to zero. Only at locations close to him some secrecy remains. The high power differences between Alice's and Bob's signals cause interferences with clean symbols and, thus, lead to rising secrecy capacities in Bob's proximity.

In our experiment with Eve in the vicinity of one of the keying nodes, we keep the WARP boards representing Alice and Bob in the same setup as in the MITM scenario, but move Eve's node close to Alice. In this setup, the distance between Alice and Bob remains 2.40 m, while Eve is 1.00 m away from Alice and 2.60 m away from Bob. Hence, Eve overhears Bob's signal with more attenuation than Alice's. Due to the asymmetry of this setup, we need to distinguish between both directions of data transmission. In particular, we consider the cases, (1) when Alice is transmitting while Bob is jamming and (2) the other way around when Bob is transmitting while Alice is jamming. The secrecy capacities highly depends on transmission direction. In a transmission from Alice to Bob, Eve is less affected by jamming than in a transmission the other way around. This is observable in the detection rates and secrecy capacities depicted in Figure 13. While achieving a satisfying detection rate for both transmission directions, Eve cannot perfectly suppress the secrecy when residing close to a jamming node. Taking a location close to any of the keying nodes might be unfavorable for eavesdropping on a mutual transmission.



(a) Secrecy capacity using a single antenna.

(b) Secrecy capacity using two antennas.

Figure 12: Maximum achievable secrecy capacity in simulation in dependency of Eve's distances to Alice and Bob. We consider a unidirectional transmission from Alice to Bob.

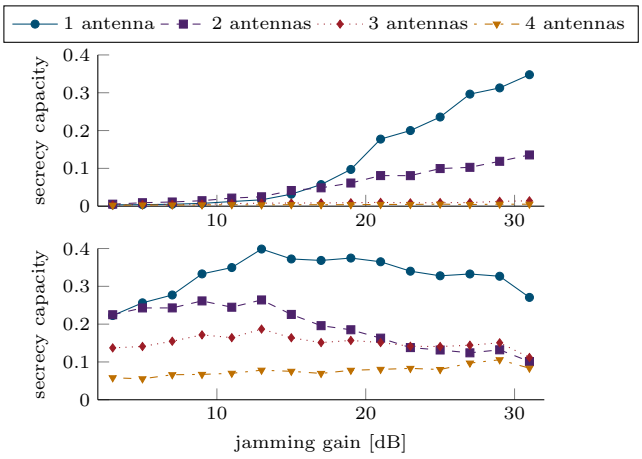


Figure 13: Secrecy capacity with Eve located close to Alice in transmission from Alice to Bob (top) and from Bob to Alice (bottom) using 16-QAM modulated signals (testbed).

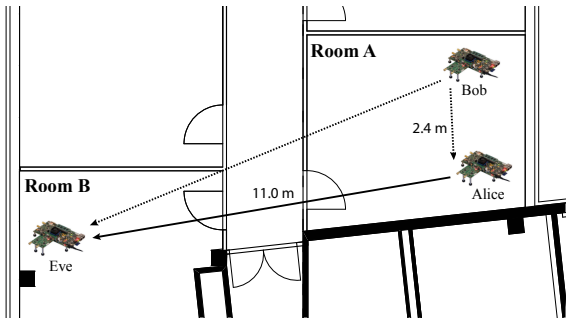


Figure 14: Experimental setup showing a typical eavesdropping scenario in an office environment.

5.10 Eavesdropping from far-away

Moving Eve to a different room illustrates a typical eavesdropping scenario in office environments. As seen in Figure 14 Alice and Bob reside in one office room, while Eve is placed in another room on the opposite part of the corridor. Due to the higher distance to the keying parties, Eve over-

hears the signals of Alice and Bob with high attenuation, hence, noise effects are more serious. Noise decreases the channel capacity also in optimal reception. Thus, the detection rates and secrecy capacities cannot achieve values as good as those in the scenarios above. As shown in Figure 15, we still observe the effects of multiple eavesdropping antennas, that increase the number of correctly detected samples and significantly decrease the secrecy of the scheme. We achieve a detection rate of up to 0.80 by using four antennas and decrease the secrecy capacity in average by 83.8% instead of using a single antenna. Although we cannot obtain perfect results, our eavesdropping attack suitably decreases the secrecy even then when Eve resides further away from the keying nodes.

5.11 Summary and Impact

With our results, we demonstrate the feasibility of our detection scheme. We significantly decrease the secrecy capacity of the key exchange, which implies an inappropriate amount of necessary repetitions to transmit a key securely. As shown in Figure 16, the multi-antenna eavesdroppers enforces the protocol to be executed around 300 times in the MITM scenario to achieve an optimal secrecy capacity of 1. With the single-antenna eavesdropper a comparable secrecy is achieved at only a few repetitions. Hence, we argue that this need of extensive privacy amplification is impractical.

Our measurements show that Eve is most powerful, when she resides centered between Alice and Bob. The more antennas Eve uses, the better her attack performance is. In the case when Eve is close to either of Alice and Bob or far away, we also observed an increase in attack performance by using multiple antennas. However, an equal distance between Eve and both keying parties (as in the MITM scenario) maximizes the eavesdropping performance.

Based on these results, we conclude that (1) our detection scheme enables attackers to successfully eavesdrop on the key exchange, (2) the attackers performance increases with the number of antennas, and that (3) eavesdroppers best reside directly in between both keying parties. These findings imply that the investigated physical layer key exchange mechanisms cannot prevent multi-antenna attackers from eavesdropping on the exchanged key. They might successfully obtain the shared secret and decrypt confidential communications.

6. CONCLUSION AND FUTURE WORK

In this work, we analyze the secrecy of a representative physical layer security scheme that utilizes artificial interference to obfuscate the exchange of a key by letting the receiver jam random samples of the transmitted signal. As high constraints on the eavesdropper are set in the original paper, we first strengthen the adversary model and equip the eavesdropper with multiple antennas. This leads to a more realistic communication scenario and increases the chances to extract confidential information from the communication between the keying parties. In our security analysis, we show the reduced protection provided by the key exchange scheme. To achieve this, the eavesdropper reveals differences in the jamming signals by comparing the simultaneous receptions at different antennas. Due to multi-path propagation, the interference of the jamming signal with the useful signal depends on the location of the receiving antennas. Based on this finding, we design an algorithm to distinguish

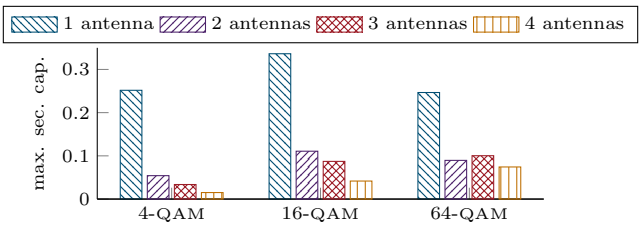


Figure 15: Maximum achievable detection rate and secrecy capacity with Eve located in another office room using different modulation schemes (testbed).

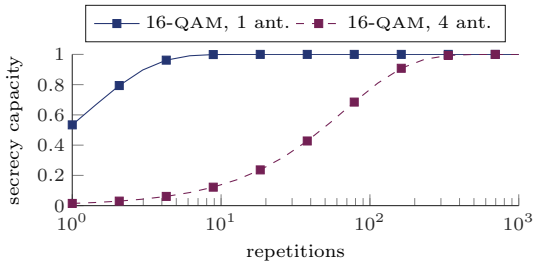


Figure 16: Cumulated secrecy capacity over number of protocol repetitions in the MITM scenario (testbed).

between clean and jammed signal parts and, thereby, figuratively 'pick the lock' to reveal the exchanged secret.

To validate our findings, we perform simulations and practical experiments in our software-defined radio (SDR) testbed, which is based on the wireless open-access research platform (WARP). We demonstrate that multi-antenna eavesdroppers massively decrease the secrecy during the key exchange and easily outperform single-antenna ones. Hence, we emphasize the need for considering strong adversaries when designing new physical layer protocols.

As future work, we plan to investigate limitations of our attack and harden the security scheme. Our attack assumes different channels between the eavesdropper and the keying parties. This is typically true for indoor WLAN communication that includes rich multi-path propagation and high antenna spacing. However, communications on larger frequencies (e.g. 802.11ad at 60 GHz) experience less multi-path effects, and those on lower frequencies (e.g. near field communication (NFC) at 13.56 MHz) have wavelengths that are larger than the distance between devices. These scenarios require further research on the secrecy of key exchange. Promising improvements of the key exchange might be based on orthogonal jamming [3] or channel randomization [12] to obfuscate even clean signals at multiple antennas.

7. ACKNOWLEDGMENTS

This work was supported by the German Federal Ministry of Education and Research (BMBF) within EC SPRIDE, by the German Research Foundation (DFG) within the Collaborative Research Centers (SFBs) CROSSING and MAKI, as well as by the Hessian LOEWE excellence initiative within CASED.

8. REFERENCES

[1] WARP Project. *http://warpproject.org.*

[2] R. Ahlswede and I. Csiszar. Common randomness in information theory and cryptography. i. secret sharing. *IEEE Transactions on Information Theory*, 39:1121–1132, 1993.

[3] N. Anand, S.-J. Lee, and E. Knightly. Strobe: Actively securing wireless communications using zero-forcing beamforming. In *Proc. 31st IEEE International Conference on Computer Communications (INFOCOM)*, pages 720–728, 2012.

[4] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener. Robust key generation from signal envelopes in wireless networks. In *Proc. 14th ACM Conference on Computer and Communications Security (CCS)*, pages 401–410, 2007.

[5] J. Barros and M. Rodrigues. Secrecy capacity of wireless channels. In *Proc. IEEE International Symposium on Information Theory (ISIT)*, pages 356–360, 2006.

[6] D. Chen, Z. Qin, X. Mao, P. Yang, Z. Qin, and R. Wang. SmokeGrenade: An efficient key generation protocol with artificial interference. *IEEE Transactions on Information Forensics and Security*, 8:1731–1745, 2013.

[7] J. Croft, N. Patwari, and S. K. Kasera. Robust uncorrelated bit extraction methodologies for wireless sensors. In *Proc. 9th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, pages 70–81, 2010.

[8] L. Dong, Z. Han, A. Petropulu, and H. Poor. Cooperative jamming for wireless physical layer security. In *Proc. 15th IEEE/SP Workshop on Statistical Signal Processing (SSP)*, pages 417–420. 2009.

[9] C. Erceg, L. Schumacher, and P. Kyritsi. IEEE P802.11 Wireless LANs: TGn channel models, 2004.

[10] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu. They can hear your heartbeats: Non-invasive security for implantable medical devices. In *Proc. ACM Special Interest Group on Data Communication (SIGCOMM) Conference*, pages 2–13, 2011.

[11] S. Gollakota and D. Katabi. Physical layer wireless security made fast and channel independent. In *Proc. 30th IEEE International Conference on Computer Communications (INFOCOM)*, pages 1125–1133, 2011.

[12] P. Huang and X. Wang. Fast secret key generation in static wireless networks: A virtual channel approach. In *Proc. 32nd IEEE International Conference on Computer Communications (INFOCOM)*, pages 2292–2300, 2013.

[13] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy. On the effectiveness of secret key extraction from wireless signal strength in real environments. In *Proc. 15th ACM International Conference on Mobile Computing and Networking (MobiCom)*, pages 321–332, 2009.

[14] D. J. C. MacKay. *Information Theory, Inference, and Learning Algorithms*. Cambridge University Press, 1st ed. edition, 2003.

[15] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik. Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel. In *Proc. 14th ACM International Conference on Mobile Computing and Networking (MobiCom)*, pages 128–139, 2008.

[16] U. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39:733–742, 1993.

[17] N. Patwari, J. Croft, S. Jana, and S. Kasera. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. *IEEE Transactions on Mobile Computing*, 9:17–30, 2010.

[18] I. Safaka, C. Fragouli, K. Argyraki, and S. Diggavi. Creating shared secrets out of thin air. In *Proc. 11th ACM Workshop on Hot Topics in Networks (HotNets)*, pages 73–78, 2012.

[19] I. Safaka, C. Fragouli, K. Argyraki, and S. Diggavi. Exchanging pairwise secrets efficiently. In *Proc. 32nd IEEE International Conference on Computer Communications (INFOCOM)*, pages 2265–2273, 2013.

[20] T. Schmidl and D. Cox. Robust frequency and timing synchronization for OFDM. *IEEE Transactions on Communications*, 45:1613–1621, 1997.

[21] M. Schulz, A. Loch, and M. Hollick. Practical known-plaintext attacks against physical layer security in wireless MIMO systems. In *Proc. Network and Distributed System Security (NDSS) Symposium*, 2014.

[22] N. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun. On limitations of friendly jamming for confidentiality. In *Proc. IEEE Symposium on Security and Privacy (SP)*, pages 160–173, 2013.

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

[24] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 1975.

[25] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam. Information-theoretically secret key generation for fading wireless channels. *IEEE Transactions on Information Forensics and Security*, 5:240–254, 2010.

[26] K. Zeng, D. Wu, A. Chan, and P. Mohapatra. Exploiting multiple-antenna diversity for shared secret key generation in wireless networks. In *Proc. 29th IEEE International Conference on Computer Communications (INFOCOM)*, pages 1–9, 2010.