Investigation of signal and message manipulations on the wireless channel

Investigation of Signal and Message Manipulations on the Wireless Channel

Christina Pöpper, Nils Ole Tippenhauer, Boris Danev, and Srdjan Capkun

Department of Computer Science, ETH Zurich, Switzerland
{poepperc,tinils,bdanev,capkuns}@inf.ethz.ch

Abstract. We explore the suitability of Dolev-Yao-based attacker models for the security analysis of wireless communication. The Dolev-Yao model is commonly used for wireline and wireless networks. It is defined on abstract messages exchanged between entities and includes arbitrary, real-time modification of messages by the attacker. In this work, we aim at understanding and evaluating the conditions under which these real-time, covert low-energy signal modifications can be successful. In particular, we focus on the following signal and message manipulation techniques: symbol flipping and signal annihilation. We analyze these techniques theoretically, by simulations, and experiments and show their feasibility for particular wireless channels and scenarios.

Keywords: Wireless Security, Adversarial Interference, Signal Manipulation

1 Introduction

In wireless radio communications, message transmissions from a sender to one or several receivers take place over the wireless channel. Given that this channel is an open and shared medium, the communication is inherently exposed to threats related to eavesdropping and intentional interference. The security analysis of wireless systems usually evaluates these intrinsic threats with respect to specific application and system properties (e.g., mobility, device complexity). As a result, a range of attacker models and corresponding assumptions arise in practical evaluations.

Certain attacker models only consider passive (eavesdropping) attacks [10,36]. Others are restricted to denial-of-service (DoS) jamming attacks in which the receiver is precluded from retrieving and decoding the signal transmitted by the sender, e. g., in military [19, 20] and increasingly in civilian [14, 35, 38] contexts. In stronger attacker models, the attacker does not only have the ability to jam (i. e., block) the original transmission, but she can also insert her own self-composed or replayed signals (insertion/ pollution attack) [1,26,28,32]. The attacker usually achieves this by either transmitting a signal with significantly more power, which "overshadows" the original transmission (this was, e. g., reported for GPS signals in [32] and for wireless access points in [26]) or by blocking the legitimate signal by jamming and then inserting her own signal at another time or on another frequency channel (e. g., demonstrated for WLAN in [28]). In both cases, in a successful attack, the receivers get deceived into receiving the inserted signal of the attacker instead of the original signal.

The strongest attacker models (e. g., in [11, 16, 24, 25]) adhere to a Dolev-Yao [5] model, in which the attacker has the capability to eavesdrop, modify, compose, and (re)play any messages transmitted and received by authorized devices. In this model, in addition to eavesdropping and insertion, the attacker can fully [24] or partially [11, 16, 25] modify and annihilate signals at the receiver's antenna.

Since attacker models are the foundation of the security analysis of any system, they should be based on a realistic assessment of the system vulnerabilities and attacker capabilities. Weaker attacker models usually underestimate the threats because they do not consider the full set of techniques that may be available to a determined attacker. For example, any jamming detection based on the energy observed on the channel could be circumvented if the attacker is using low-energy signals that corrupt only the message preamble; many standard receivers would not be able to decode the message, although the data part of the message would remain unchanged. On the other hand, the strongest attacker models are often not motivated by practical considerations. For example, Dolev-Yao based models will allow the attacker to transfer information to remote locations instantaneously while this is not realistic [22]. Although designing a system with an overestimation of the attacker capabilities does not harm the security of the system, it may complicate the proposed solutions and create unnecessary overhead on the communication or make the hardware setup more costly.

To investigate the suitability of different attacker models for wireless communication, in this work we explore the basic techniques for wireless signal (message) manipulations and investigate their assumptions and practical realization. We first categorize physical-layer techniques available to strong attackers and show how they affect the received message at the logical layer. We then focus on techniques that allow the attacker to achieve covert, low-energy manipulations during the signal transmission. More specifically, we investigate *symbol flipping* attacks, by which the attacker can change symbols of the transmitted message and thus attack the message integrity, and *signal annihilation* attacks, by which the attacker suppresses the sender's signal at the receiver.

In short, our main contributions are as follows:

- We categorize adversarial interference in wireless transmissions and compare it to the capabilities of a Dolev-Yao attacker.
- We present a theoretical model to describe symbol flipping attacks.
- We explore the effectiveness of symbol flipping and signal strength manipulation (annihilation) attacks in simulations and validate our findings experimentally using USRP [6] devices.

The remainder of this paper is organized as follows: In Section 2, we describe related work and state the problem that we tackle. In Section 3, we define and classify adversarial interference in wireless communications and analyze its mapping to the Dolev-Yao attacker model. We analyze symbol flipping attacks and the conditions for their success theoretically in Section 4. In Section 5, we evaluate the feasibility of symbol flipping and signal strength manipulation attacks by simulations and experiments. We discuss implications of our findings in Section 6 and conclude the paper in Section 7.

2 Related Work and Problem Statement

2.1 Related Work on Signal Manipulations

Wireless communication jammers have been widely analyzed and categorized in terms of their capabilities (e.g., broadband, narrowband, tone) and behavior (e.g., constant, sweep, random, reactive) [13, 19, 38]. Jammer models used in prior works [13, 31, 38] cover the interference with transmissions by signal jamming and dummy packet or preamble insertions. The authors of [25, 30] explicitly consider signal modification, overshadowing, and symbol flipping in their respective attacker models and propose solutions that achieve jamming- (and overshadowing-)resistant communication. However, neither of the mentioned works investigates the *feasibility* of such attacks.

When signals collide, the stronger one may survive regardless of the kind of signal. Whitehouse et al. [33] propose a technique for sensor networks to detect and recover packets from (unintended) collisions taking advantage of the *capture* effect, whereby the packet with the stronger signal strength can be received in spite of a collision. [23] quantifies the SINR conditions under which the capture effect can be observed. Another example is GPS tampering by *overriding* [3]; the success of the attack is based on the fact that GPS receivers tune in to the strongest (four) GPS signals available. The authors of [9] point out that GPS signals can also be subject to spoofing and flipping attacks that succeed with a certain probability. While they do not derive these probabilities, our findings in the experimental evaluation are conform to their numbers.

The authors of [1, 21] show that for low-power wireless devices (sensor motes) predictable and deterministic symbol corruptions (flippings) are hard to achieve by mote-class attackers. In these papers, the authors describe the effect of intentional interference with a signal transmission in terms of the predictability of bit and packet corruptions. Our work is related to this, however, we do not restrict our investigations to customary sensor mote attackers but explore the underlying principles and conditions under which message manipulations and signal annihilation can be successful.

2.2 Problem Statement

In this paper, we address the following problem: *How can an attacker actively interfere with ongoing wireless transmissions and which success rates can be achieved?* This question aims at exploring the feasibility of real-time manipulations of signals (messages) in which the attacker tampers with the signals *while they are being transmitted*.

In particular, we will practically investigate two types of attacks that may allow the attacker to (i) modify signals and the data content of messages during their transmission or (ii) disrupt the communication in a covert, hard-to-detect manner. We briefly outline these two types of attacks:

Symbol flipping targets the data payload or the packet preamble, trying to modify the packets at the receivers. Flipped symbols in the preamble prevent both the decoding of the data payload and the detection of the jamming attack on standard devices because they do not allow the receiver to detect the beginning of the message header or result in a misinterpretation of the constellation diagram. Successful preamble corruption does not require that *specific* symbols are flipped. Although integrity measures (e. g., checksums

and CRCs) may identify symbol flippings, they will not succeed if the attacker can deterministically change bits of the CRC to conceal her modifications. We note that a number of wireless protocols do not employ integrity protection measures or do not enforce them cryptographically (such as WEP 802.11, civilian GPS, or the RFID-M1 communication protocol).

Signal annihilation can be achieved when the attacker's signal creates destructive interference with the sender's signal at the receiver (similar to multipath interference [29]). In this case, the sender's signal gets attenuated and may be annihilated at the receiver; hence the receiver cannot detect an ongoing transmission. This attack can be performed without prior knowledge of the message content and is difficult to prevent without resorting to hardware modifications of the transceivers. Signal attenuation and amplification attacks are also crucial to the security of RSSI-based localization [8].

The investigation of the research question above examines realistic attacker capabilities that are assumed in a number of works on wireless communication without exploration, e. g. in [11, 16, 24, 25]. We therefore see our work as an important building block for constructing realistic threat models and appropriate countermeasures. This is specially relevant in view of the recent development of tools that practically interfere with ongoing transmissions and show the feasibility of real-time reactive radio interference, such as [34].

3 Classifying Wireless Attacks

Attacker models used in the security analysis of wireless protocols are often defined on an abstract layer. They usually consider effects—such as deletion and modification—that an attacker can have on the reception of *messages* at the receiver. We will explain such an attacker model in more details in Section 3.1.

In the context of wireless systems, message-based attacker models have been adopted in a number of works, e. g., in [11, 15, 16, 22, 24, 25]. In these works, the attacker is usually assumed to be able to eavesdrop, insert, modify, replay, delay, or delete any *signal* being transmitted on the wireless channel. Since messages are defined on the abstract, logical level of bits and signals comprise also the physical characteristics of the transmission, it is not clear that abstract network protocol attacker models can be applied directly to wireless communications.

In the following, we summarize message-layer effects commonly used in abstract attacker models and identify signal-layer effects which cause them (Section 3.1). To model these effects, we define *adversarial interference* as attacks in which the attacker transmits her own signals to the channel and we investigate how this can be captured in existing physical-layer reception models (Section 3.2). We then formally classify attacks based on adversarial interference (Section 3.3).

3.1 Signal Manipulations and Effects on Messages

In attacker models such as the Dolev-Yao (DY) model [5], the attacker's capabilities include eavesdropping and the arbitrary modification and deletion of messages transmitted by legitimate entities as well as the composition and insertion of the attacker's

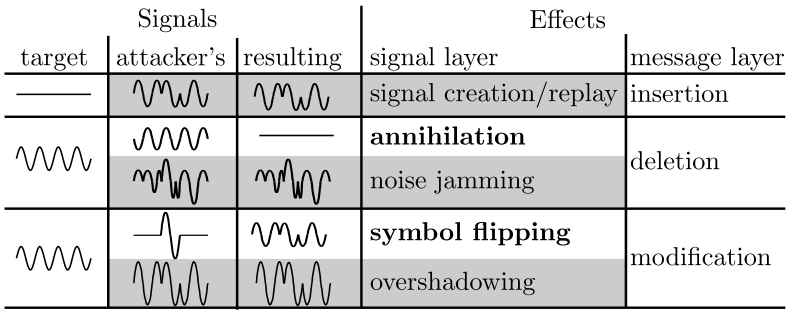

Fig. 1. Examples of signal-layer manipulations and their effects on the message layer. Signals can, e. g., be annihilated or jammed, their signal strength can be modified, and their amplitude, phase or frequency can be changed to influence their demodulation. Message-layer effects can in general be caused by multiple signal-layer effects. Signal-layer effects in bold will be investigated in Section 4.

own messages at the receivers. In the following, we list the effects that a DY-like attacker is assumed to be capable of achieving at the victim's receiver and give examples of how a wireless attacker can cause these effects on the signal layer (see Figure 1).

Message Eavesdropping: The attacker can observe all messages sent to one or more receivers. In a wireless network, on the signal layer, an attacker can observe the channel and record all signals with own antennas. The interpretation of the received signals as messages may require secrets such as the used spreading codes, which might not be available to the attacker. In some scenarios, the attacker can be restricted in the number of channels that she can simultaneously monitor [4, 25, 37].

Message Insertion and Replay: The attacker acts like a legitimate member of the network, and as such she can insert messages or replay previously received messages. In wireless networks, this is a reasonable assumption on both the message and signal layer because the attacker can construct own messages and transmit the corresponding signals and she can also replay previously received signals and messages. Restrictions on this can exist, e. g., in spread spectrum communication using secret sequences shared between the sender and receivers [19].

Message Deletion: The attacker is in control of the network and can prevent the reception of messages. To achieve this effect on a wireless channel, several methods can be used on the signal layer. These methods include jamming of complete messages using higher energy noise signals as well as jamming only the message preamble to hide it from the receiver. A more covert attack is to annihilate the signal by sending inverse signals to the receiver. While these methods all have the same effect on the message layer, i. e., the deletion of the message, in each method the receiver will capture different signals on the (physical) signal layer.

Message Modification: The attacker can modify the messages obtained by the receivers. To modify wireless messages, the attacker can either change the signals during their transmission by adding own signals—thus influencing the demodulation of single

symbols (*symbol flipping*)—or prevent the receiver from obtaining the original message (message deletion) and then insert a modified version of the message.

Signal-layer manipulations such as attenuation and amplification are not directly reflected in abstract attacker models. If the signal amplitude of the message is increased or decreased (within a certain threshold), the data content on the message layer will remain unchanged with most modulation schemes. However, the amplitude change can be relevant for a number of wireless protocols, e. g., RSSI-based localization [8] for which signal strength amplification and attenuation constitute an attack.

3.2 Model of Adversarial Interference

In this section, we present a model to describe the possible effects that signal-layer manipulations can have on the message layer.

We start with a brief system description and introduction of the notation used. We consider a sender A and a particular receiver B that are able to communicate over a wireless radio link. Wireless transmissions are characterized by the messages (data) being transmitted and the physical signals used to transmit the data. The physical signals are determined by the used modulation scheme, power levels, etc. Let $s(t)$ be the signal transmitted by A; $s(t)$ is the result of the encoding process at A that packages, error-encodes, and modulates a data sequence $\mathbf{S}_A$. Let $\hat{s}(t)$ be the signal that B receives under unintentional interference (including noise and signal attenuation). In order to receive the message, B applies a function $d(\cdot)$ to demodulate $\hat{s}(t)$; it outputs the demodulated symbol sequence $\mathbf{S}$. If B does not detect the message on the channel[1], the demodulation results in the empty symbol sequence $\emptyset$.

Let $j(t)$ be the signal transmitted by an attacker J and $\hat{j}(t)$ be the corresponding signal received at B. The demodulation of $\hat{j}(t)$ at B results in $d(\hat{j}(t)) = \mathbf{S}_J$. We now define adversarial interference as follows:

Definition 1. *Let $\hat{o}(t)$ be the superposition of two signals $\hat{s}(t)$ and $\hat{j}(t)$ at B. Let $\mathbf{S}_A = d(\hat{s}(t))$, $\mathbf{S}_A \neq \emptyset$. Let $\mathbf{S}_B = d(\hat{o}(t))$ at B. The transmission of $j(t)$ is an* interference attack *if $\mathbf{S}_B \neq \mathbf{S}_A$ or if $P_{\hat{o}}(t) \neq P_{\hat{s}}(t)$, where $P_{\hat{o}}(t)$ and $P_{\hat{s}}(t)$ are power metrics for $\hat{o}(t)$ and $\hat{s}(t)$.*

This definition implies that, in a successful interference attack, the attacker changes the message symbols and/or the signal power of the original signal $\hat{s}(t)$. We note that $\hat{s}(t)$ and $\hat{j}(t)$ must overlap in time and frequency band at B for the attack to succeed.

The defined signal-layer manipulations can be integrated in existing physical reception models for wireless communications, see Appendix A. This integration supports and facilitates the identification of different types of attacks.

3.3 Classification

Given the considerations above, we can identify the following types of attacks based on adversarial interference. We also map them to message-layer effects, see Figure 1. We use the notation as introduced in Definition 1.

[1] The detection of a signal may, e.g., not be triggered if the signals power lies below a threshold or if its preamble does not match the used protocol.

- **Symbol flipping**: One or more symbols of $\mathbf{S}_A$ are flipped. $\hat{o}(t)$ gets demodulated into a valid sequence $\mathbf{S}_B$, $\mathbf{S}_B \neq \mathbf{S}_A$ and $\mathbf{S}_B \neq \mathbf{S}_J$. $P_{\hat{o}}(t) \approx P_{\hat{s}}(t)$ for the message duration.
- **Amplification**: $\hat{j}(t)$ amplifies $\hat{s}(t)$ at B. $\mathbf{S}_B = \mathbf{S}_A$. $P_{\hat{o}}(t) > P_{\hat{s}}(t)$ for the entire signal $\hat{o}(t)$.
- **Attenuation**: $\hat{j}(t)$ attenuates $\hat{s}(t)$ at B. $\mathbf{S}_B = \mathbf{S}_A$. $P_{\hat{o}(t)} < P_{\hat{s}(t)}$ for the entire signal $\hat{o}(t)$.
- **Annihilation**: $\hat{o}(t)$ falls below the noise level. $\hat{s}(t)$ is removed at B by a (sufficiently close) inverse jamming signal $\hat{j}(t) \approx \hat{s}^{-1}(t)$. $\mathbf{S}_B = \emptyset$. $P_{\hat{o}}(t) \ll P_{\hat{s}}(t)$ for the entire signal $\hat{o}(t)$.
- **Overshadowing**: $\hat{s}(t)$ appears as noise in the much stronger signal $\hat{j}(t)$. $\mathbf{S}_B = \mathbf{S}_J$. $P_{\hat{o}}(t) \gg P_{\hat{s}}(t)$ for the entire signal $\hat{o}(t)$.
- **Noise jamming**: $\hat{j}(t)$ is noise to prevent B from detecting the message, thus blocking its reception. $\mathbf{S}_B = \emptyset$. $P_{\hat{o}}(t) \gg P_{\hat{s}}(t)$ for the entire signal $\hat{o}(t)$.

Amplification, attenuation, and annihilation can be denoted as *signal strength modification* attacks. From the attacker's point of view, a similar action is performed in all attack cases listed above, namely the transmission of a signal $j(t)$. What differs are the type and strength of $j(t)$ and its dependency on $s(t)$: While $j(t)$ is independent of $s(t)$ in overshadowing and noise jamming attacks, the attacker uses $s(t)$ to construct $j(t)$ in signal strength modification attacks and both $s(t)$ and $o(t)$ in symbol modification attacks, where $o(t)$ is the signal that the attacker wants B to receive.

We note that, according to Definition 1, attacks in which the attacker jams the original signal and inserts an adversarial signal with a shift in time or frequency band (e.g., exploiting the channel structure of WLAN 802.11 signals by transmitting on separate frequencies [28]) are a combination of adversarial interference and a parallel insertion/pollution attack [12, 25].

4 Theoretical Analysis of Symbol Flipping

In this section, we focus on symbol modification attacks and present our model of symbol flipping. We restrict our considerations to single carrier modulations and reason about flipping on the level of symbols. We distinguish symbol flipping attacks according to the attacker's goal. $\mathbf{S}_A$, $\mathbf{S}_B$, and $j(t)$ are as in Definition 1.

Definition 2. *A* deterministic symbol flipping attack *has the goal to make B demodulate $\mathbf{S}_B = \mathbf{S}_T$, where the symbol sequence $\mathbf{S}_T \neq \mathbf{S}_A$ has been defined by the attacker before the transmission of $j(t)$. A* random symbol flipping attack *targets at modifying any symbol(s) of $\mathbf{S}_A$ such that $\mathbf{S}_B \neq \mathbf{S}_A$.*

In the following, we denote the symbols of the sequence $\mathbf{S}_A$ also as *target symbols*. Deterministic symbol flipping requires a-priori knowledge about the target symbols, i.e., about the parts of a message that are to be flipped. We next investigate how to achieve successful symbol flipping.

The way multiple signals get superimposed depends on their modulations (including signal power, phase shifts, etc.). We consider linear digital modulation schemes such as 2-PAM, 4-QAM (QPSK), and 16-QAM, which divide the constellation space into

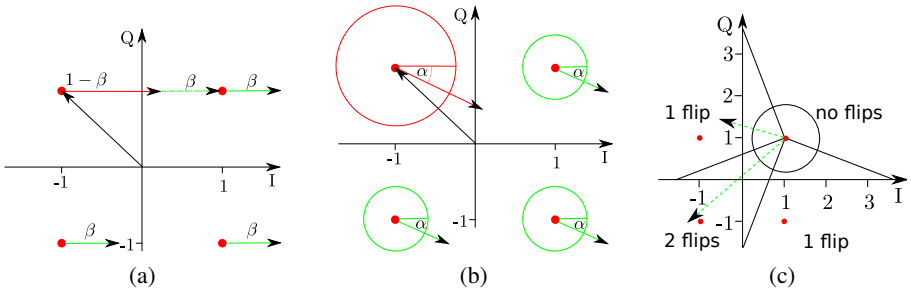

Fig. 2. (a) Effect of imperfect baseband alignment of the flipping symbol w.r.t. the target QPSK symbol. Given a delay βT_s, the fraction β of the energy will be added to the next symbol. (b) Effect of the relative carrier phase offset α between the target and the flipping signals. The phase offset rotates the energy contribution of the flipping signal. As all flipping symbols have the same carrier phase offset, all energy contributions get rotated. (c) Depending on the signal energy and rotation, different constellation regions can be reached by symbol flipping.

decision regions with varying sizes and shapes. For QPSK (see Figure 2a), the decision regions are separated by the axes of the IQ-plane. Given a modulation scheme and the received signal vector $\hat{s}$, the decision element in the receiver's decoder outputs the constellation point with the minimum Euclidean distance (ML detection) [20]. Moving a signal vector $\hat{s}$ in the constellation implies a change in signal power (distance from the origin of the constellation diagram) and/or a changed angular phase of the signal. For QPSK, we define two ways of flipping a symbol (this will later matter for our simulations):

Definition 3. *For QPSK, a* short transition *denotes the shift of a symbol vector into an adjacent constellation region (ideally parallel to the I- or Q-axis). A* long transition *denotes a diagonal shift into the opposite constellation region.*

In Gray-encoded constellations, a short transition changes one bit of a symbol and a long transition both bits of the symbol. Such transitions can be caused by adding a QPSK symbol with modified carrier phase alignment and enough power. If this symbol temporally overlaps with one or more target symbols, we call it *flipping symbol*.

In practice, three factors influence the result of a symbol flipping attack: (i) the baseband alignment of the sender's and attacker's symbols, (ii) the relative carrier phase offset of the attacker's signal, and (iii) the energy of the attacker's symbol.

(i) The *baseband alignment* of the flipping symbols determines the amount of energy that will not be contributed to the target but to the *neighboring* symbols in the message. Here, we assume a sequence of flipping symbols that are all delayed by the same time βT_s, where T_s is the symbol duration. Then, a fraction β of the energy will influence the decoding of the following symbol. Figure 2a visualizes the effect of the baseband symbol alignment and shows the effect on the next target symbol: the misaligned flipping symbol, represented by the vector (2,0), will affect the current symbol $(-1,1)$ with $1-\beta$ and the following symbol with β. A similar effect may occur to the current symbol due the prior flipping symbol. We will analyze the required baseband alignment by simulations and experiments in Section 5.

(ii) In addition to the effect of the baseband alignment, the relative *carrier phase offset* α of the flipping signal with respect to the target signal will rotate the energy contribution of the signal. As all flipping symbols have the same carrier phase offset, all energy contributions get rotated in the same way, see Figure 2b.

(iii) For short transitions, the minimum required *signal energy* (for exact carrier phase and baseband alignment) is a factor $1/\sqrt{2}$ of the energy of the target signal; for long transitions, at least as much energy as in the target signal is required. Figure 2c gives an example of a short transition (one bit changed) and a long transition (two bits changed). Based on our model, we can predict the probability of successful symbol flipping for a random carrier phase offset. Figure 3 displays the analytical flipping probabilities depending on the relative signal energy, derived using trigonometrical functions.

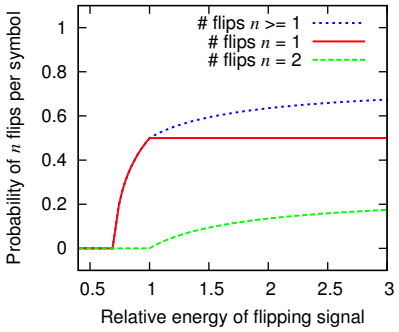

Fig. 3. Analytical probability of successful symbol flipping for random carrier phase alignment and perfect baseband alignment, depending on the relative signal energy.

5 Simulation and Experimental Evaluation

In this section, we explore the conditions for successful symbol flipping and signal annihilation (as defined in Section 3.3) under an attacker as presented in Section 5.1. We verify our theoretical symbol flipping model of Section 4 by simulations in Matlab [27] in Section 5.2. The main results are then validated using signals captured from recorded wireless communications in Section 5.3. We also explore signal annihilation and attenuation by experiments with wireless devices in Section 5.4.

5.1 Simulation Setup and Attacker Model

Simulation setup. For our simulation and experimental evaluation of symbol flipping and annihilation, we focus on QPSK modulation due to its widespread use (e.g., in 802.11 and Bluetooth 3.0). We implemented an 802.11 digital QPSK modem with an AWGN channel. The matched filter g(t) was implemented by a root raised cosine filter. The carrier frequency was fixed to $f_c = 2.4$ GHz with $\phi_1(t) = \cos(2\pi f_c t)$ and $\phi_2(t) = -\sin(2\pi f_c t)$ for the I and Q channels, respectively. Figure 7 in Appendix B displays the simulation setup.

Our simulations are based on 1000 random QPSK symbols that we use to create the flipping symbols. For long transitions, we invert each symbol and double its amplitude; for short transitions we combine the inverted symbol with its complex-conjugate. We use the following notations: The original (target) symbol is denoted by $\mathcal{T}$, the short transition flipping symbol by $\mathcal{S}$, and the long transition flipping symbol by $\mathcal{L}$. $\mathcal{R}$ is a flipping symbol with random carrier phase offset and same power as $\mathcal{L}$.

Attacker model. In our simulations, we focus on two attacker types: (a) a *strong attacker* with perfect carrier phase alignment, able to predict which symbols are going to be sent, and therefore using perfect flipping signals; (b) a *weak attacker* without carrier phase alignment and therefore random flipping signals. The goal of the strong attacker is to perform a *deterministic* symbol flipping attack, while the weak attacker tries to perform a *random* symbol flipping attack (see Definition 2). In order to achieve their goals, the attackers follow these strategies:

- The strong attacker uses a short transition flipping signal $\mathcal{S}$ to flip a specific bit of a target symbol. To flip both bits of the symbol, she uses a (more powerful) long transition flipping signal $\mathcal{L}$. In both cases, the flipping signals have *perfect carrier phase alignment* with the target signal.
- The weak attacker uses flipping symbols $\mathcal{R}$ with the same power as $\mathcal{L}$ but with *random carrier phase* (rotating the signal vector in the IQ-plane) with respect to the target signal.

We note that a short transition by a strong attacker is successful only if the *intended* bit was flipped, while for a weak attacker the flipping of any of the two bits (or both bits) of the symbol are considered a success.

5.2 Simulated Modification of Modulated Signals

Following our model from Section 4, we will now predict the effects of varying power, carrier phase offset, and baseband offset of the flipping signal. Finally, we will predict their impact on annihilation attacks.

Power of the Flipping Signal. According to our model, the power of the flipping signal needs to be greater than a fraction $1/\sqrt{2}$ of the target signal. Flipping in this case is only successful if the flipping signal has the optimal phase (e.g., shifts the symbol (1,1) into the direction of (1,-1)). For random phases, the power of the flipping signal must be higher.

Figure 4a displays the influence of the relative power of the flipping signal on the probability to flip QPSK symbols (for random carrier phases of the flipping signal and perfect baseband symbol alignment). The plot shows the probability of a random symbol flip for a weak attacker and a deterministic flip for a strong attacker, for an SNR level of 20 dB. The weak attacker has no carrier phase synchronization and thus no control over the angle of the flipping signal. The strong attacker uses a flipping signal with perfect phase synchronization.

The simulation confirms that, for a low noise level (high SNR), the power $P_{\mathcal{S}}$ of a short transition symbol must satisfy $P_{\mathcal{S}} \geq \frac{P_{\mathcal{T}}}{\sqrt{2}}$, where $P_{\mathcal{T}}$ is the power of the target symbol, in order to change a single bit of the symbol. The weak attacker's probability to flip a single bit converges towards 50 % for $P_{\mathcal{R}} \geq P_{\mathcal{T}}$ and her chance to flip both bits of a symbol towards 25 % for $P_{\mathcal{R}} \to \infty$ (not shown in Figure 4a).

Carrier Phase Offset for Symbol Flipping. The carrier phase offset between the target signals and the flipping signals at the receiver is hard to control for the attacker. This is the main reason why symbol modification attacks are difficult to conduct even with perfect advance knowledge of the data to be sent. The effect of a constant carrier phase offset under noise is displayed in Figure 4b for $P_{\mathcal{R}} = P_{\mathcal{L}} = 2P_{\mathcal{T}}$, $P_{\mathcal{S}} = \sqrt{2}P_{\mathcal{T}}$, and 20 dB SNR.

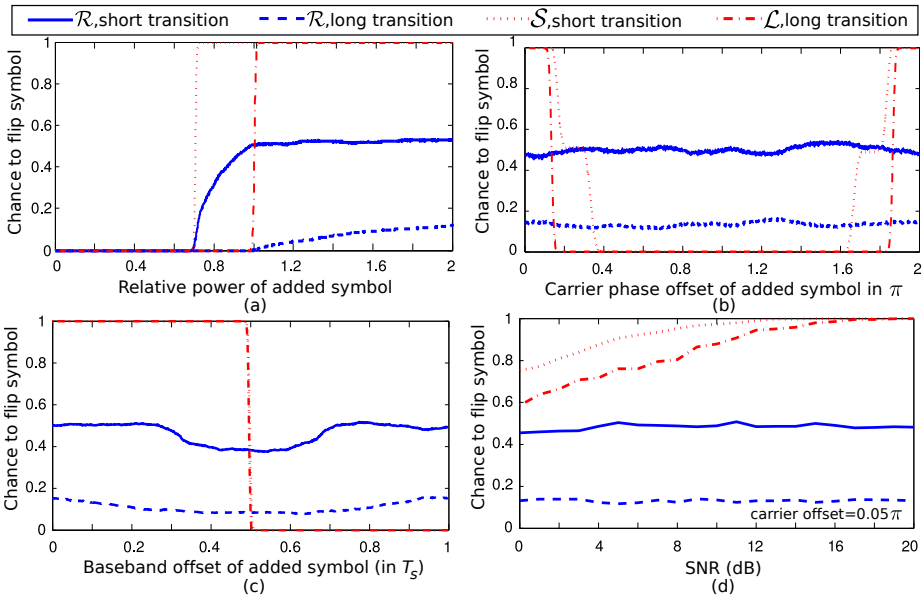

Fig. 4. Influence of the flipping symbol on the probability to change a QPSK symbol using a random-phase flipping symbol $\mathcal{R}$ (weak attacker) or a perfect short/long flipping symbol ($\mathcal{S}/\mathcal{L}$) (strong attacker). (a) Influence of the relative power of the flipping symbol. (b) Influence of the carrier phase offset of the flipping signal. (c) Influence of the baseband offset (relative to the symbol duration T_s) of the flipping symbol. (d) Influence of the SNR for a fixed carrier phase offset of 0.05π.

Simulations without noise show that a strong attacker must hit the carrier phase within about $13.5\,\%$ of the carrier phase duration to flip both bits of the target symbol (long transition). Short transitions for the strong attacker require less carrier phase precision, the tolerance is $25\,\%$. The carrier phase offset has no impact for a weak attacker because she uses flipping signals with random phase; the carrier phase offset does therefore not influence her probability to flip bits.

If the attacker does not synchronize correctly to the sender's carrier *frequency*, this will make it almost impossible for her to predict the optimal carrier phase alignment for the flipping symbols. However, the attacker must synchronize the carrier frequency of her flipping signals only once to a target transmission, which will then result in the same carrier phase offset for all flipping signals with respect to the target transmission.

Baseband Offset for Symbol Flipping. A weak attacker might have problems aligning the flipping symbols correctly to the target symbols. This has the effect that the energy of the flipping symbol will not only contribute to the target symbol but also influence neighboring symbols (see Section 4). We evaluated the impact of this baseband offset by simulations, see Figure 4c. We set $P_{\mathcal{R}} = P_{\mathcal{L}} = 2P_{\mathcal{T}}$ and $P_{\mathcal{S}} = \sqrt{2}P_{\mathcal{T}}$ as before for the power of the flipping signals and 20 dB SNR. The simulation results show that the probability for a *weak* attacker to flip a bit degrades smoothly. In Figure 4c, her

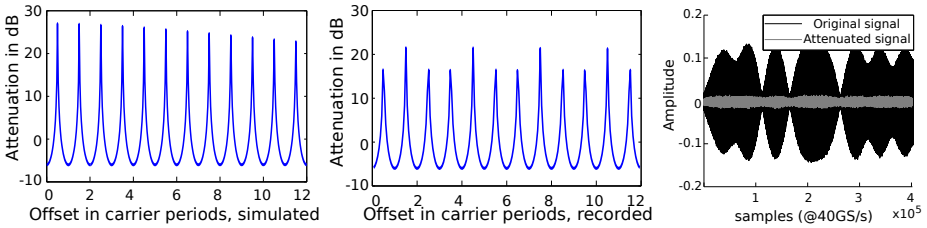

Fig. 5. Signal annihilation attack. Figures (a) and (b) depict the signal attenuation obtained by adding the same signal delayed with different carrier offsets. (a) shows the results using signals simulated in Matlab (with an SNR of 30 dB), (b) uses recorded signals (measured SNR of around 30 dB). (c) shows the practical signal attenuation obtained using our experimental carrier.

probability does not converge to zero for a baseband misalignment of one symbol duration (T_s) because the following symbol is flipped (which is a success for the weak attacker). The strong attacker has a probability of 1 to flip both bits of a symbol if the baseband offset is smaller than 50 % (with sufficiently high SNR).

Similarly to the carrier frequency offset, an offset in the baseband symbol *rate* between the attacker and the sender will lead to changing baseband offsets for a sequence of flipping symbols, which will not influence the weak attacker but make deterministic attacks for the strong attacker almost impossible.

Influence of the SNR. We next investigate the influence of the Signal-to-Noise-Ratio on the attacker's probability to perform successful symbol flipping. Intuitively, the higher the SNR at the receiver, the better a strong attacker can predict the effects of the flipping attack. To demonstrate the effect of the SNR on the attacker's success probability, we ran a simulation with $P_{\mathcal{R}} = P_{\mathcal{C}} = 2P_{\mathcal{T}}$, $P_{\mathcal{S}} = \sqrt{2}P_{\mathcal{T}}$, carrier phase offset 0.05π, and perfect baseband alignment. The results in Figure 4d show that the SNR does not influence the weak attacker, but lower SNR values require the strong attacker to have a more accurate carrier phase synchronization to flip the target.

Simulation of Signal Strength Modification. We now investigate *signal annihilation* attacks (cp. Section 3.3). For this purpose, we use the legitimate signal of the sender to attenuate the sender's signal at the receiver by destructive interference, similar to worst-case effects in multipath environments. The attacker's goal is to attenuate the overall power of the signal so that it is not detected at the receiver (instead of changing the message content). Since this attack repeats the signals transmitted by the sender, it is agnostic to the actual data content of the message; the attacker does not need to know it in advance. The repeated signal will also have the same carrier frequency as the original signal, eliminating this possible source of randomness for the attacker. To fully annihilate the original signal, the attacker's signal needs to have the same power as the sender's signal at the receiver.

Figure 5a shows the simulated signal attenuation at the receiver for variable delays between the transmitted (original) and the repeated (adversarial) signal using the simulation setup in Section 5.1 with an SNR of 30 dB. The highest attenuation of ap-

proximately 28 dB is achieved only when shifting by a delay of π and high attenuation is reached every 2π of the carrier delay. This high attenuation slightly decreases for higher offsets in carrier periods due to the resulting larger time offset between the two signals. We refer to this attack as a π-shift-attack. We note that the original signal can also be amplified instead of attenuated. This would occur when shifting by a delay of 2π and multiples of it. The original signal could be amplified by up to 6 dB.

Given that the π-shift-attack does not require demodulation or complex logic at the attacker, it can be implemented using only directional antennas and possibly an amplifier. In Section 5.4, we present a practical implementation of this attack and show that high attenuation is also possible in practice.

5.3 Simulated Modification of Recorded Signals

We continue our evaluation with signals transmitted over the air and recorded by an oscilloscope. This allows us to validate the simulation results of symbol flipping and signal attenuation (Section 5.2) with a non-ideal transceiver and lossy communication channel. In our experiment, we combine our digital QPSK modem with the capabilities of a universal software radio peripheral (USRP [6]). We use fully modulated messages in a frame that closely resembles the 802.11b frame specification [2] with a preamble for carrier frequency offset estimation and synchronization [17]. Figure 8 in Appendix C displays our setup for the experimental investigations in Sections 5.3-5.4.

Symbol Flipping of Recorded Signals. Our main goal of this experiment is to validate our predicted probabilities for an attacker using optimal $\mathcal{S}/\mathcal{L}$ flipping symbols to reach her goal with random carrier phase synchronization. In addition, we are interested in the chance of a weak attacker flipping any (neighboring) bits. We simulated the addition of the recorded flipping symbol with varying baseband offsets of 0, $0.25T_s$, and $0.5T_s$ and averaged carrier phase offsets between 0 and 2π. The power of the flipping symbols is $P_{\mathcal{R}} = P_{\mathcal{L}} = 2P_{\mathcal{T}}$, $P_{\mathcal{S}} = \sqrt{2}P_{\mathcal{T}}$ as in the previous simulations.

Table 1 compares the chances for successful attacks on the target symbol (T) and (unwanted) flipping of neighboring symbols (N) between the results of simulation without noise (Sim) and the findings based on our recorded signals (Recorded). We observe that the predicted probabilities for long and short transitions closely follow the probabilities computed from the recorded signals for baseband offsets of 0 and $0.25T_s$. The influence on the target and neighboring symbols only differ for an offset of $0.5T_s$. This is most likely due to the fact that the probabilities to symbol flipping at $0.5T_s$ occupy a transition region (Figure 4c) and thus can take different values in the presence of noise. Nevertheless, our main result is confirmed by the experimental evaluation: about 13 % flipping

Table 1. Probability of modifications of the target (T) and neighboring (N) symbols in simulated vs. recorded signals for random carrier phase offset (%).

	Baseband Offset					
	0		$0.25 \times T_s$		$0.5 \times T_s$	
Sim	T	N	T	N	T	N
$\mathcal{R}$, short	25	0	25	0	0	0
$\mathcal{R}$, long	13.5	0	9.3	0	0	49.96
$\mathcal{R}$, *any*	63.5		59.3		74.82	
Recorded	T	N	T	N	T	N
$\mathcal{R}$, short	24.3	0	25.0	0	21.5	9.7
$\mathcal{R}$, long	11.1	0	11.1	0	2.8	27.8
$\mathcal{R}$, *any*	58.3		58.3		70.8	

chance for long transitions and about 25 % for a short transition, both with random carrier phase offset and small baseband offset.

Signal Annihilation of Recorded Signals. We used recorded messages as described in 5.3 to simulate the effect of signal annihilation by adding time-shifted copies of the signal. The lower plot in Figure 5 shows the obtained attenuation. In comparison to the simulation with ideal signals (i.e., upper plot in Figure 5), the achieved highest attenuation was lower by few decibels. Correct demodulation at the receiver was still not possible with our implementation, hence the signal was successfully annihilated. We also observe that there are several possible carrier offsets at which this high attenuation can be achieved.

5.4 Experimental Evaluation of Signal Annihilation

The main goal of this evaluation is to estimate how accurately the carrier phase offset can be controlled and what attenuation could be achieved in real multipath environments. For this purpose, we built the experimental signal annihilation setup shown in Figure 8 (Appendix C). The setup consists of a transmitter (USRP), a receiver (oscilloscope), and two directional antennas (with a gain of 15 dBi) connected by a cable. One antenna is directed at the transmitter and the second antenna repeats the received signal towards the receiver. The USRP sends periodic signals, which are simultaneously repeated by the antennas, received at the oscilloscope, and demodulated in Matlab. To achieve signal annihilation, the amplitude and carrier phase delay of the attacker's signal must closely match the legitimate signal at the receiver. We controlled the carrier phase offset between the transmitted and repeated signals by changing the distance between the antennas. Since we used high gain directional antennas, we could also adapt the power of the repeated signal by directing the antenna away from the receiver by some degrees. For a distance of 2 m between the USRP and the receiver and an appropriate positioning of the directional antennas (approximately 1 m away from the line of sight), we achieved the predicted signal attenuation down to the noise level. Figure 5c shows the signals received at the oscilloscope with and without the two directional antennas. Our results show an attenuation of approximately 23 dB. By using a longer (1 m) cable between the directional antennas, we also verified that the resulting higher baseband offset between the transmitted and repeated signals does have a significant impact on the achieved attenuation. We note that for longer distances, the same setup would require additional amplification between the directional antennas.

5.5 Summary of Results

We evaluated the influence of carrier and baseband offsets, amplitude mismatches, and the SNR on symbol flipping, first theoretically in Section 4 and then by simulations and experiments. Our findings show that, given accurate carrier phase and baseband synchronization, deterministic symbol flipping is feasible for strong attackers.

If the attacker cannot adapt to the sender's carrier phase offset, a random offset will allow her to achieve long transitions causing deterministic symbol flippings in around 13.5 % of the cases; for a short transition, this chance reaches up to 25 % (see Table 1). The weak attacker aiming at changing one bit of any symbol will achieve this with a

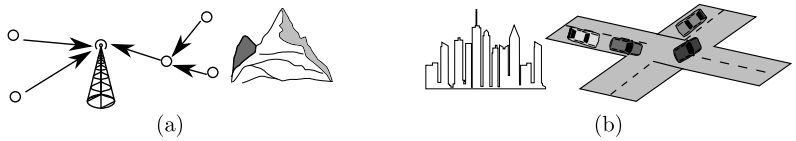

Fig. 6. Examples for wireless networks. (a) Static networks in quasi-static, quasi-free-space environments allow a strong attacker to perform deterministic signal manipulations; we thus confirm the Dolev-Yao model as an appropriate worst-case attacker model. (b) Environments with multipath effects and networks with mobile nodes suggest that deterministic, covert signal manipulations are hard to achieve—a probabilistic attacker model is more realistic.

chance of 50 % (see Figure 4 and Table 1) per flipping symbol as long as her signal has enough power, regardless of the carrier phase offset and baseband offset. Since the carrier phase offset is influenced by the channel and the geometric setup of the sender, attacker, and receiver, it might be hard to exactly match the target offset in practice. We discuss the impact of this on deterministic message manipulations in Section 6.

We also predicted an attenuation of the original signal to the noise level by adding the same signal shifted by a certain carrier phase offset for realistic SNR levels (e.g., 20 dB). We reproduced the attenuation with recorded signal traces in Matlab and showed its practical feasibility in a lab environment using two directional antennas.

We discussed the use of rotated and scaled QPSK symbols as flipping signals. The use of alternative, e.g., shorter symbols of higher bandwidth, is left for future work.

6 Implications

In the previous sections, we have investigated the practicability of low-energy symbol flipping and signal annihilation attacks through simulations and experiments. We will now discuss the implications of our results in selected scenarios.

In a first scenario, we consider a wireless network with static wireless nodes and quasi-static, quasi-free-space channel properties. An example of such a network could be wireless sensor nodes deployed in rural areas, see Figure 6a. If an attacker with strong signal manipulation capabilities is allowed to access any location, she can measure distances and estimate the channel with high precision to any target node. The attacker would thus be able to achieve carrier phase synchronization and control the signal amplitude levels at the target receiver in order to flip symbols and/or annihilate transmitted signals with very high probability (for our system with non-coherent receivers). This corresponds to the model of our strong attacker (Section 5.1).

In a number of scenarios that are typical for wireless network deployments at least one of the assumptions in the above case is violated. Examples include static wireless networks in dynamic environments (e.g., urban areas) or mobile wireless networks, see Figure 6b. In both examples, wireless nodes communicate over time-varying fading channels [29]. This channel makes carrier phase synchronization and amplitude control at the target receiver very difficult (if not infeasible) for the attacker as it requires her to know the state information of the sender-receiver channels. Given that feedback signaling is typically needed for channel state information (CSI) estimation [18], it is hard to

launch deterministic attacks without receiver cooperation. Failing to do so significantly reduces the probability of a strong attacker to perform deterministic short and long symbol flipping (Definitions 2 and 3) to 25% and 12.5%, respectively (in our scenario using QPSK modulation).

Furthermore, our results show that an attacker without a priori knowledge of the transmitted data has a chance of up to 75 % (see Table 1) to change *any* symbol (flip one or two bits) by adding a flipping symbol with twice the signal power. Depending on the error-correcting mechanisms employed at the receiver, this can allow the attacker to jam messages (or message preambles) in an energy-efficient way.

In summary, we draw the following conclusions: We conclude that the attacker models selected for the security analysis of wireless communication need to be chosen in accordance with the deployed network and scenario. In the worst case, the attacker can covertly and deterministically delete and manipulate messages if the wireless network deployment cannot guarantee that the channel is dynamic. These attacks would not be detected by existing energy-based jamming detection countermeasures, as they do not add significantly more energy on the channel. In this aspect, the attacker's capabilities become very close to those of the Dolev-Yao model. If a dynamic channel can be assumed, even the strongest attacker can only probabilistically delete and modify messages without risking detection by energy-based jamming detection techniques. Such a probabilistic attacker model captures dynamic time-varying channels in the sense that the carrier phase offset is likely to change between individual messages. We note that the probability with which the attacker will be successful depends on a number of system parameters, including coherency or non-coherency of the reception process of the receiver, multipath effects, etc. We leave the investigation of these settings open for future work.

7 Conclusion

In this paper, we investigated the applicability of abstract attacker models of wireline protocols in the security analysis of wireless protocols. We first categorized different types of signal-layer attacks and mapped them to the Dolev-Yao attacker model. Then we explored the feasibility of basic techniques for manipulating wireless signals and messages. We focused on symbol flipping and signal annihilation attacks that both allow covert, low-energy manipulations of signals during their transmission. Our theoretical analysis, simulations, and experiments identified their conditions for success for QPSK-modulated signals and showed their practical feasibility given quasi-static, quasi-free-space channels. Our findings confirm the need of strong attacker models (similar to Dolev-Yao's model) in specific static scenarios, but they also suggest to construct alternative, probabilistic attacker models for a number of common wireless communication scenarios.

Acknowledgments

This work was partially supported by the Zurich Information Security Center. It represents the views of the authors.

References

1. Anish Arora and Lifeng Sang. Capabilities of low-power wireless jammers. In *IEEE Infocom Miniconference*, 2009.
2. IEEE Standards Association. *IEEE Standard 802.11b-1999: Wireless LAN MAC and PHY Specifications*, 1999. `http://standards.ieee.org`.
3. Sherri Davidoff. GPS spoofing. `http://philosecurity.org/2008/09/07/gps-spoofing`, 2008.
4. Yvo Desmedt, Rei Safavi-Naini, Huaxiong Wang, Chris Charnes, and Josef Pieprzyk. Broadcast anti-jamming systems. In *Proceedings of the IEEE International Conference on Networks (ICON)*, 1999.
5. Danny Dolev and Andrew C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.
6. Ettus. Universal software radio peripheral (USRP). `http://www.ettus.com`.
7. Piyush Gupta and P. R. Kumar. The capacity of wireless networks. *IEEE Transactions on Information Theory*, 46(2), 2000.
8. Jeffrey Hightower, Gaetano Borriello, and Roy Want. SpotON: An indoor 3D location sensing technology based on RF signal strength. Technical Report 2000-02-02, University of Washington, 2000.
9. Todd E. Humphreys, Brent M. Ledvina, Mark L. Psiaki, Brady W. O'Hanlon, and Paul M. Kintner Jr. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In *Proceedings of the ION GNSS International Technical Meeting of the Satellite Division*, 2008.
10. Suman Jana, Sriram Nandha Premnath, Mike Clark, Sneha Kumar Kasera, Neal Patwari, and Srikanth V. Krishnamurthy. On the effectiveness of secret key extraction from wireless signal strength in real environments. In *Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*, 2009.
11. Tao Jin, Guevara Noubir, and Bishal Thapa. Zero pre-shared secret key establishment in the presence of jammers. In *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*. ACM Press, 2009.
12. Chris Karlof, Naveen Sastry, Yaping Li, Adrian Perrig, and Doug Tygar. Distillation codes and applications to DoS resistant multicast authentication. In *Proceedings of the Network and Distributed Systems Security Symposium (NDSS)*, 2004.
13. Mingyan Li, Iordanis Koutsopoulos, and Radha Poovendran. Optimal jamming attacks and network defense policies in wireless sensor networks. In *Proceedings of the IEEE Conference on Computer Communications (InfoCom)*, 2007.
14. Guevara Lin and Guolong Noubir. On link layer denial of service in data wireless LANs: Research articles. *Wireless Communications & Mobile Computing*, 5(3):273–284, 2005.
15. An Liu, Peng Ning, Huaiyu Dai, and Yao Liu. Defending DSSS-based broadcast communication against insider jammers via delayed seed-disclosure. In *Proceedings of Annual Computer Security Applications Conference (ACSAC)*, 2010.
16. Yao Liu, Peng Ning, Huaiyu Dai, and An Liu. Randomized differential DSSS: Jamming-resistant wireless broadcast communication. In *Proceedings of the IEEE Conference on Computer Communications (InfoCom)*, 2010.
17. Alan V. Oppenheim, Ronald W. Schafer, and John R. Buck. *Discrete-Time Signal Processing*. Prentice-Hall Signal Processing Series, 2nd edition, 1998.
18. Antonio Pascual Iserte. *Channel state Information and joint transmitter-receiver design in multi-antenna systems*. PhD thesis, Polytechnic University of Catalonia, 2005.
19. Richard A. Poisel. *Modern Communications Jamming Principles and Techniques*. Artech House Publishers, 2006.

20. Richard A. Poisel. *Foundations of Communications Electronic Warfare*. Artech House Publishers, 2008.
21. Lifeng Sang and Anish Arora. Capabilities of low-power wireless jammers. Technical Report OSU-CISRC-5/08-TR24, The Ohio State University, 2008.
22. Patrick Schaller, Benedikt Schmidt, David Basin, and Srdjan Čapkun. Modeling and verifying physical properties of security protocols for wireless networks. In *Proceedings of the IEEE Computer Security Foundations Symposium*, 2009.
23. Dongjin Son, Bhaskar Krishnamachari, and John Heidemann. Experimental study of concurrent transmission in wireless sensor networks. In *Proceedings of the ACM Conference on Networked Sensor Systems (SenSys)*, 2006.
24. Mario Strasser, Boris Danev, and Srdjan Čapkun. Detection of reactive jamming in sensor networks. *ACM Transactions on Sensor Networks*, 7:16:1–16:29, September 2010.
25. Mario Strasser, Christina Pöpper, Srdjan Čapkun, and Mario Čagalj. Jamming-resistant Key Establishment using Uncoordinated Frequency Hopping. In *Proceedings of the IEEE Symposium on Research in Security and Privacy (S&P)*, 2008.
26. Symantec. Securing enterprise wireless networks. White Paper, 2003.
27. The MathWorks, Inc. Matlab – a numerical computing environment. `www.mathworks.com`.
28. Nils Ole Tippenhauer, Kasper Bonne Rasmussen, Christina Pöpper, and Srdjan Čapkun. Attacks on Public WLAN-based Positioning. In *Proceedings of the ACM Conference on Mobile Systems, Applications and Services (MobiSys)*, 2009.
29. David Tse and Pramod Viswanath. *Fundamentals of wireless communication*. Cambridge University Press, 2005.
30. Mario Čagalj, Jean-Pierre Hubaux, Srdjan Čapkun, Ramkumar Rengaswamy, Ilias Tsigkogiannis, and Mani Srivastava. Integrity (I) Codes: Message Integrity Protection and Authentication Over Insecure Channels. In *Proceedings of the IEEE Symposium on Research in Security and Privacy (S&P)*, 2006.
31. Mario Čagalj, Srdjan Čapkun, and Jean-Pierre Hubaux. Wormhole-based antijamming techniques in sensor networks. *IEEE Transactions on Mobile Computing*, 6(1):100–114, 2007.
32. J. S. Warner and R. G. Johnston. Think GPS Cargo Tracking = High Security? Think Again. *Technical report, Los Alamos National Laboratory*, 2003.
33. Kamin Whitehouse, Alec Woo, Fred Jiang, Joseph Polastre, and David Culler. Exploiting the capture effect for collision detection and recovery. In *Proceedings of the IEEE workshop on Embedded Networked Sensors (EmNets)*, 2005.
34. Matthias Wilhelm, Ivan Martinovic, Jens Schmitt, and Vincent Lenders. Reactive jamming in wireless networks: How realistic is the threat? In *Proceedings of the forth ACM conference on Wireless network security (WiSec)*, 2011.
35. Anthony D. Wood and John A. Stankovic. Denial of service in sensor networks. *IEEE Computer*, 35(10):54–62, 2002.
36. Liang Xiao, Larry Greenstein, Narayan Mandayam, and Wade Trappe. Fingerprints in the ether: Using the physical layer for wireless authentication. In *Proceedings of the IEEE International Conference on Communications (ICC)*, 2007.
37. Wenyuan Xu, Wade Trappe, and Yanyong Zhang. Channel surfing: defending wireless sensor networks from jamming and interference. In *Proceedings of the ACM Conference on Networked Sensor Systems (SenSys)*, 2006.
38. Wenyuan Xu, Wade Trappe, Yanyong Zhang, and Timothy Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2005.

A Integration into the SINR Model

In the physical SINR model [7], the transmission from a node A is successfully received by node B under simultaneous transmissions from a set $\{I_i\}$ of transmitters if

$$\frac{P_{AB}}{N + \sum_i P_{iB}} \geq \beta_B, \tag{1}$$

where $P_{AB} = P_{\hat{s}(t)}$ and P_{iB} are the sender's and the transmitters' signal powers at B, respectively, N is the ambient noise level, and β_B is the minimum SINR (Signal to Interference plus Noise Ratio) required for successful message reception at B. The SINR model represents the reception of the original transmission $s(t)$ under concurrent signals of sufficient or insufficient power.

In order to capture adversarial interference in the SINR model, we split the overall interference into legitimate (neighboring) transmissions and interference from an attacker J. Let $P_{JB} = P_{\hat{j}(t)}$ denote J's signal power at B (originating from one or multiple collaborating attackers). In order to reflect different types of adversarial interference, we distinguish constructive and destructive interference. We denote by P^c_{JB} the fraction of P_{JB} that creates constructive interference with $\hat{s}(t)$, by P^d_{JB} the fraction of P_{JB} that creates destructive interference with $\hat{s}(t)$, and by P^n_{JB} the fraction of P_{JB} that appears as noise at B; $P^c_{JB} + P^d_{JB} + P^n_{JB} = P_{JB}$. B receives a signal of sufficient power to enable demodulation for $P_{AB} + P^c_{JB} - P^d_{JB} > 0$ if

$$\frac{P_{AB} + P^c_{JB} - P^d_{JB}}{N + \sum_i P_{iB} + P^n_{JB}} \geq \beta_B. \tag{2}$$

The left-hand side of Equation 2 is the power of the signal $\hat{o}(t)$ at B. Based on this equation, we can distinguish the following cases:

- $P^d_{JB} = P_{AB} + P^c_{JB}$:
  This attack annihilates the signal with $d(\hat{o}(t)) = \emptyset$.
- $P^n_{JB} \gg P_{AB} + P^c_{JB}$:
  This results in noise jamming with $d(\hat{o}(t)) = \emptyset$.
- $P^c_{JB} - P^d_{JB}$ is in the order of P_{AB} and P^n_{JB} does not cause a blocked message at B:
  This can modify (flip) bits in the message and we get $d(\hat{o}(t)) \neq \emptyset$ and $d(\hat{o}(t)) \neq \mathbf{S}_A$. If this happens in the packet preamble we get $d(\hat{o}(t)) = \emptyset$.
- P^c_{JB} and P^d_{JB} do not modify the demodulation result and P^n_{JB} does not block the reception at B:
  In this case, we get $d(\hat{o}(t)) = d(\hat{s}(t)) = \mathbf{S}_A$, possibly under an amplified (with $P^c_{JB} > P^d_{JB}$) or attenuated (with $P^c_{JB} < P^d_{JB}$) signal.
- $P^c_{JB} - P^d_{JB} \gg P_{AB}$ and P^n_{JB} does not cause a blocked message at B:
  In this case, B will demodulate $d(\hat{o}(t)) = d(\hat{j}(t)) = \mathbf{S}_J$, hence the attacker's message is overshadowing the message from A.

B Simulation setup

Figure 7 shows the simulation setup used for the Matlab simulations. The modulated data symbols are passed through a matched filter g(t) (root raised cosine) and up-converted to the carrier frequency (2.4 GHz band) (ϕ(t)). The channel is simulated by adding Gaussian noise (AWGN). After sampling with rate kT_s, a Maximum Likelihood (ML) decoder outputs the decoded symbols.

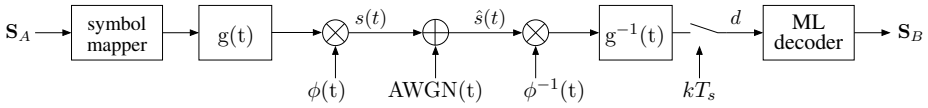

Fig. 7. Simulation setup used for the Matlab simulations.

C Experimental setup

Figure 8 shows the setup we used for our practical experiments. Symbols are generated by a QPSK modulator and form the input to a USRP that transmits them over the air. We capture the original or manipulated transmissions using an oscilloscope. We then demodulate and analyze the data.

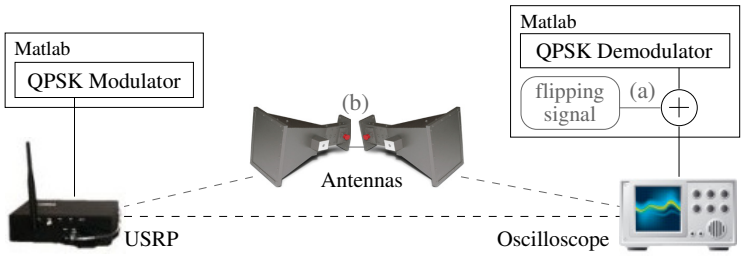

Fig. 8. Experimental setup. (a) For simulated symbol flipping of recorded signals, we add the flipping signals to the captured signals in Matlab. (b) For the experiments on signal attenuation, two antennas capture and repeat the signals.