Towards a Cryptographic Model for Wireless Communication

Frederik Armknecht and Christian Müller
University of Mannheim, Mannheim, Germany

Keywords: Wireless Communication, Attacker Model, Physical Properties, Distance Bounding, Friendly Jamming.

Abstract: The Man-in-the-Middle Model (MitMM) is commonly used in cryptography for modeling an attacker in multi-party scenarios. It essentially assumes that the attacker fully controls the communication between all parties, i. e., can stop and modify messages at her discretion. We argue that this model is too strong for realistically capturing the case of wireless communication. In consequence, schemes that exploit properties of wireless communication such as friendly jamming or distance bounding, cannot be analyzed in a common framework. Moreover, the lack of an appropriate model hinders the development of new schemes. Given the ever-increasing importance of wireless communication, e. g., in the context of the Internet of Things, we propose a new formal model for wireless communication. Starting from the formal MitMM, we identify three key aspects — communication channels, signals, and locality — that are not represented, explain how to extend the model accordingly, and propose a tailored WCM. Based thereon, we explain how these limit the capabilities of an attacker in the form of a WAM. Moreover, we demonstrate for an existing security mechanism, namely friendly jamming, which is not covered by the MitMM how the new model allows for analyzing/formalizing the security.

1 INTRODUCTION

Security models are fundamental for unambiguously analyzing or proving the security of cryptographic schemes by formalizing security goals and attacker models. While the security goals may vary between different use cases, the attacker model is usually more universal. For typical scenarios involving two or more communicating parties, the so-called Man-in-the-Middle Model (MitMM) introduced by (Dolev and Yao, 1983) is commonly utilized in which the attacker is assumed to have full control over the communication, e. g., message eavesdropping, delaying, or modification.

This work at hand is motivated by the observation that the MitMM can be too strong in the case of *wireless communication*. Without doubt, considering a very strong attacker model is often necessary and useful, i. e., if certain capabilities of an attacker cannot be excluded, assume the worst case; if a mechanism provides security against a strong attacker, so does it for weaker (and potentially more realistic) attackers.

We claim, however, that the situation is different for wireless communication. First, academic and industrial research produced various security mechanisms which, regarding the security, cannot be properly addressed in the MitMM. The probably best known example are Distance Bounding (DB) protocols (e. g., (Brands and Chaum, 1994; Hancke and Kuhn, 2005)). But also other *existing* schemes cannot be analyzed adequately in the model, e. g., the shield for Implantable Medical Devices (IMDs) by (Gollakota et al., 2011), or other friendly jamming approaches (e. g., (Shen et al., 2013; Berger et al., 2014)).

Second, the development of *new* schemes is hindered: mechanisms may be rejected as they are insecure in the MitMM, while they may be secure in practice. More precisely, some assumptions made in the MitMM about the attacker's capabilities typically do not hold in wireless networks due to physical laws. For instance, a transmitted message spreads like a wave in every direction from the sender. Normally, an attacker cannot influence the wave which is on the opposite side of the sender. Also, modifying messages is not directly possible as all an attacker can do is to send signals on her own which then interfere with the other parties' signals. For example, (Pöpper et al., 2011) showed that, in wireless communication networks, reliable and targeted manipulation of messages is difficult in practice. (Avoine et al.,

Armknecht, F. and Müller, C.
Towards a Cryptographic Model for Wireless Communication.
DOI: 10.5220/0012809300003767

In *Proceedings of the 21st International Conference on Security and Cryptography (SECRYPT 2024)*, pages 249-261
ISBN: 978-989-758-709-2; ISSN: 2184-7711

2021) likewise criticize that existing formal models make impractical assumptions.[1]

Given these shortcomings, we see the benefits of a model tailored to wireless communication as an alternative to the MitMM. This is particularly true given the ever increasing relevance of wireless communication as, e. g., the Internet of Things (IoT), with a forecast of 27.0 billion IoT devices by the end of 2025 (Mohammad Hasan, 2022), connects a plethora of devices in wireless networks and over the Internet. There is a strong demand for appropriate security measures to protect IoT devices and users against misuse and malicious behavior.

Our contributions and structure of the paper are:

- In Sec. 2, we identify several properties of wireless networks that are not (or not correctly) covered by the MitMM and categorize these as *communication channels*, *signals*, or *locality*.
- Starting from the MitMM, we introduce a new model for wireless communication, dubbed Wireless Communication Model (WCM), in Sec. 3.
- In Sec. 4, we discuss how the WCM may impact an attacker's capabilities, resulting in the Wireless Attacker Model (WAM).
- We demonstrate how WCM and WAM can be used for formalizing/analyzing several existing security mechanisms that could not be properly represented by the MitMM, namely DB protocols and friendly jamming, in Sec. 5.
- Sec. 6 summarizes related work and concludes this work.

We hope the new model allows for founded and comparable security research in this important area and helps to develop novel security mechanisms that would be unthinkable in the traditional model.

2 MOTIVATION

This section motivates the need for a dedicated security model for wireless networks. First, we recall the established MitMM and highlight shortcomings regarding peculiarities of wireless communication. We categorize these as: communication channels (Sec. 2.2), signals (Sec. 2.3), and locality (Sec. 2.4). For each of these, we describe the situation in wireless networks, discuss why it is not represented in the MitMM and why it needs to be integrated, and summarize these findings as "lessons learned". The latter form the basis for our WCM introduced in Sec. 3.

2.1 The Man-in-the-Middle Model

In the following, we recall the MitMM introduced by (Dolev and Yao, 1983), using the formulation as given by (Katz, 2002). Note that we are only interested in modeling the capabilities of an attacker to intercept and modify messages that are exchanged between communicating parties.

The system in the MitMM comprises a finite set of parties Π that are modeled as Interactive Turing Machines (ITMs). In a nutshell, an ITM extends the classic probabilistic Turing machine by including (besides the work tape, random tape, and auxiliary tapes) an additional read-only communication-in (comm-in) tape and an additional write-only communication-out (comm-out) tape that allow for receiving messages from and sending messages to other ITMs, respectively. We refer to (Katz, 2002, Definition 2.1) for a full definition. The MitMM assumes that all communication between the parties in Π is under control of an attacker $\mathcal{A}$. This is captured by the notion of being *linked via* $\mathcal{A}$. As a consequence, in the MitMM, all communication between any of the parties in Π is "routed" through $\mathcal{A}$ and she may decide for any incoming message whether it will be forwarded and, if so, whether it is modified beforehand. We refer to (Katz, 2002, Definition 2.2) for a full definition.

2.2 Communication Channels

2.2.1 Description

Wireless communication utilizes a shared and open medium composed of one or several physical channels, i. e., ultimately, any communication channel is realized through *at least* one physical channel.

Examples for systems using a single *physical channel* for communication are Wireless Personal Area Networks, e. g., based on IEEE 802.15.4 (IEEE, 2011), and Wireless Local Area Networks (WLANs), e. g., WLAN with Direct-Sequence Spread Spectrum (IEEE, 1997). In contrast, mobile telephony networks, such as those based on GSM or 5G, and the satellite telephony services based on Inmarsat, utilize separate channels for sending and receiving data (Elbert, 2008).

2.2.2 Discussion

In the MitMM, each party has access to exactly *one* comm-out tape and each of these is *directly linked* to a comm-in tape of the adversary (cf. (Katz, 2002, Definition 2.2)), thus forming the *only* available communication channel to any party.

[1] More shortcomings of the MitMM in the case of wireless communication are discussed in Sec. 2.

A wireless communication channel is realized through the use of at least one physical channel. Thus, if more than one physical channel is available, *several* communication channels may be established between two parties. In fact, techniques like Frequency-Hopping Spread Spectrum (FHSS), as used for example in Bluetooth (Bluetooth SIG, 2016) and WLAN with FHSS (IEEE, 1997), cannot be expressed by using one communication channel only.

Moreover, these physical channels are *open* to anyone. In principle, messages transmitted on these channels can be received by any party that listens on the same channel. As we detail further in Sec. 2.3.2, this limits the possibilities of an attacker.

2.2.3 Lessons Learned

A wireless communication model should allow parties to establish several communication channels which are open to everyone.

2.3 Signals

2.3.1 Description

In wireless communication, messages are encoded into sinusoidal waves, using different modulation schemes. Moreover, these are sent with a certain amount of power, which a receiver perceives as so-called signal strength and which is often simply represented as Received Signal Strength Indicator (RSSI).

2.3.2 Discussion

Whenever two parties send messages at the same time on the same physical channel, these messages can *collide*. This can lead to cancellation, amplification, or other modification of the resulting signal. In fact, this is the only technical possibility for an attacker to *modify* messages.

In the MitMM, a user cannot detect whether messages sent to him have been blocked. This is no longer true for wireless communication where jamming *detection* is possible. A simple form of it relies on the RSSI, e. g., if packet errors occur during reception but the corresponding RSSI is high, then the transmission was probably jammed. This form of jamming detection has been extensively studied, e. g., by (Xu et al., 2005) or by (Grover et al., 2014) in the form of a systematic overview of jamming and detection methods.

Interestingly, jamming may also be employed for providing message confidentiality (so-called *friendly jamming*), e. g., as shown by (Gollakota et al., 2011). In their paper, they use the proximity between two devices to mitigate eavesdropping and, furthermore, utilize jamming for achieving their goal. That is, deliberately sending another signal whenever a transmission is going on renders the original message undecodable for other parties *except* for the, in this case, benign jammer, who, using the advantage of knowing the jamming signal, reconstructs the original message after all. In Sec. 5.1, we use the proposed model to formalize the security of such a friendly jamming scheme.

2.3.3 Lessons Learned

The fact that messages are modulated onto physical signals affects an attacker's capabilities, possible countermeasures, and the development of new schemes. Thus, a wireless communication model needs to cover physical signals, including signal collisions and jamming.

2.4 Locality

2.4.1 Description

When a party sends a signal at some point in time, it arrives at another party with a *time delay* that depends on the distance between sender and receiver. Moreover, the distance affects the *signal strength* of the perceived signal which eventually determines whether the recipient gets the message or not.

2.4.2 Discussion

In the MitMM, the concepts of time and space are non-existent. However, for wireless communication, the situation is different. For instance, while traveling, signals may suffer from path loss and fading, especially when running through barriers in-between. If the signal strength falls below the noise level, transmitted data may become irretrievable. This impacts the connectivity of parties *and* an attacker's capabilities to jam messages, e. g., the attacker might not receive the message she wants to jam, or the attacker's signal might be too weak to be received by the targeted party. In fact, the properties of time and space have been discussed for novel security measures in wireless systems.

In the time domain, a compelling example is the area of DB protocols, e. g., (Brands and Chaum, 1994; Hancke and Kuhn, 2005; Tippenhauer and Čapkun, 2009; Rasmussen and Capkun, 2010; Ranganathan et al., 2012; Boureanu et al., 2015; Drimer and Murdoch, 2007). These build on ideas presented by (Desmedt et al., 1988). DB protocols consider the round trip delay of (two) communicating parties, thus, providing an upper bound to their distance.

The property of space can also be utilized as a security measure. For example, ZigBee Light Link (ZigBee Alliance, 2012) uses signal strength measurements to determine *proximity* of two parties. Besides the available power for sending and receiving, the RSSI is mainly influenced by physical quantities, i. e., path loss and distance between sender and receiver. In practice, the distance is easily measurable, while the path loss varies over time and is affected by its environment and actual physical conditions, even if the distance remains constant. That is, when two parties establish a communication channel, an eavesdropper's view of that channel de-correlates rapidly with distance (Zenger et al., 2016; Eberz et al., 2012). (Hershey et al., 1995) proposed to use the physical environment to establish common *shared* information between two parties, which is unique for these two at that point in time and space.

2.4.3 Lessons Learned

In the MitMM, the attacker is omnipresent, i. e., she controls all communication. This is not given in wireless networks where an attacker's position in relation to the other parties is relevant. Even if an attacker comprises several parties at different locations, the communication between these are likewise subject to the restrictions discussed above. That is, a model should integrate the concept of relative positions of parties and the influence on the communication.

3 WIRELESS COMMUNICATION MODEL

Next, we introduce a formal model for wireless communication on the Physical Layer (PHY) of the OSI model, dubbed Wireless Communication Model (WCM). To this end, we explain how the model addresses each of the three identified aspects, i. e., channels (cf. Sec. 2.2), signals (cf. Sec. 2.3), and locality (cf. Sec. 2.4).

We stress that the aim of the model is to represent wireless communication only, i. e., parties may have further means to communicate, e. g., being directly wired. In some scenarios, it may be reasonable to add further communication tapes to the model to also cover non-wireless communication. However, such communication channels can be modeled "classically" and are hence out of scope.

3.1 Communication Channels in the WCM

We assume a set of parties Π and an attacker $\mathcal{A}$. Like in the MitMM, they are modeled as probabilistic ITMs (see (Katz, 2002, Definition 2.1)). To model the wireless communication between different parties (including $\mathcal{A}$), we likewise adopt the concept of *communication tapes*. However, there are several differences:

- Cells contain physical signals σ (cf. Sec. 3.2).
- We assume (for unique referencing of parallel activities and to capture the notion of time) a global discrete timer that divides the flow of time into time slots $t \in \mathbb{N}$ with $t+1$ following t and so on.
- We assume a system-wide parameter chs that denotes the total number of *publicly* available physical channels, and also an ordering on these channels.

Contrary to (Katz, 2002, Definition 2.2):

- We assume that *any* party $\mathcal{P}$ (including any attacker $\mathcal{A}$) has *exactly* chs comm-in and chs comm-out tapes, denoted by $(\mathsf{CT}_{\text{in}})_1^{\mathcal{P}}, \ldots, (\mathsf{CT}_{\text{in}})_{\mathsf{chs}}^{\mathcal{P}}$ and $(\mathsf{CT}_{\text{out}})_1^{\mathcal{P}}, \ldots, (\mathsf{CT}_{\text{out}})_{\mathsf{chs}}^{\mathcal{P}}$, respectively.
- $(\mathsf{CT}_{\text{in}})_i^{\mathcal{P}}$ and $(\mathsf{CT}_{\text{out}})_i^{\mathcal{P}}$ are connected to the i-th physical channel.
- The number of the attacker's comm-out tapes only depends on chs.

For any communication tape CT (either *in* or *out*), $\mathsf{CT}[j]$ denotes the j-th *cell* of this specific tape. Comm-out tapes are write-only and comm-in tapes are read-only tapes. That is, a party can write to a cell of any of its comm-out tapes and read from a cell of any of its comm-in tapes. However, reading from and writing to any cell but the current one are not possible, i. e., any party $\mathcal{P}$ (including $\mathcal{A}$) can only read or write to the t-th cell where t denotes the current time slot.[2]

The reason for this design decision is that the tapes model the physical channels used for communication. Reading or writing correspond to eavesdropping on and demodulating signals or sending modulated signals on these frequencies. Once a signal passed a party, it cannot be eavesdropped on anymore. Once a signal is sent, this action cannot be taken back.

Furthermore, any party can only access one cell at the same time, i. e., it can either read from *or* write to a *single* communication tape. The motivation for this design decision is as follows. In cryptography,

[2] There are no restrictions on *storing* data read from a tape in the past or preparing data to be written in the future.

parties are commonly modeled as Turing machines which in turn model single task algorithms. For technical reasons, sending and receiving at the same time or accessing several physical channels require separate devices. Thus, a party in our model represents the smallest processing unit that may operate on its own. Note that we do not exclude that, in practice, an attacker may have access to several physical channels at the same time. However, formally this would be expressed by several parties that interact with each other, possibly using some non-wireless communication channels. Like in the MitMM, this is not particularly expressed within the model but it is straightforward to include this.

We stress that, in our model, we assume each physical channel to be *loosely* synchronized with the global timer in the sense that a communication tape's cell corresponds exactly to the duration of one signal period of the underlying carrier frequency. In other words, each communication channel moves forward with the same speed as the others.

3.2 Signals in the WCM

Communication parties are usually oblivious to the fact that, on the PHY, signals are used to transport the messages. However, as discussed in Secs. 2.3 and 2.4, physical signals may interfere or be delayed which eventually impacts the messages received by the parties. Given that the main intention of the proposed model is to express the capabilities of an attacker to impact wireless communication, we discuss the connection between physical signals on the one hand, and the messages sent and received by parties on the other hand in the following.

3.2.1 Physical Signals

Physical signals are commonly represented by sinusoidal waves, e. g., formalized as

$$A(t) \cdot \sin(2\pi f t + \varphi(t)) \tag{1}$$

with the following parameters: the *amplitude* $A \in \mathcal{R}_{\geq 0}$ (correlated to the signal strength), the *frequency* $f \in \mathcal{R}_{>0}$ ($1/f$ gives the signal's period), and the *phase shift* φ with $0 \leq \varphi < 2\pi$ (the phase shift of the signal compared to a non-shifted sine signal). Consequently, we model a signal σ by this triple of parameters.

Definition 1 (Signals and Signal Space)**.** *A* signal σ *is defined as* $\sigma = (A, f, \varphi) \in \Sigma$ *where* $\Sigma = \mathcal{R}_{\geq 0} \times \mathcal{R}_{>0} \times [0;2\pi)$ *denotes the* signal space.

The term 0 *refers to the signal with* $A = 0$*.*

In our model, σ refers to the information about a physical signal stored in one slot of a communication tape. That is, it represents the state of a signal during a particular time slot. We consider all components of σ to be constant for the duration of one time slot, which is why the amplitude A and the phase shift φ are represented as scalars rather than time-dependent functions. Practically, 0 refers to the case that no signal is present. In particular, an *empty cell* contains this term.

As signals are considered to be periodic, one can phase-shift any signal by shifting the signal along the time axis. Formally, we introduce the Shift operation for for this.

Definition 2. *The* Shift *operation changes the phase of a given signal by a given parameter. It is defined as* $\mathsf{Shift} : [0;2\pi) \times \Sigma \to \Sigma$*. Let* $\varphi_0 \in [0;2\pi)$ *be a phase shift value and* $\sigma = (A, f, \varphi) \in \Sigma$ *a signal, then,*

$$\begin{aligned}\mathsf{Shift}(\varphi_0, \sigma) &:= \mathsf{Shift}_{\varphi_0}(\sigma) \\ &:= \left(A, f, \varphi + \varphi_0 - \left\lfloor \frac{\varphi + \varphi_0}{2\pi} \right\rfloor \right).\end{aligned} \tag{2}$$

3.2.2 Modulation and Demodulation

When two parties are communicating, they usually exchange messages composed of *message symbols* $\mu \in M$ where M denotes the message alphabet. Technically, this requires to transform message symbols into physical signals (modulation) and vice versa (demodulation), being defined as follows.

Definition 3 (Modulation and Demodulation)**.** *The* modulation function Mod *converts a message* μ *into a sequence of* ρ *signals to be sent over the air. It takes as input a message symbol* $\mu \in M$ *and the signal strength parameter* $s \in \mathcal{R}_{>0}$ *and encodes these into* ρ *signals* $\sigma_1, \ldots, \sigma_\rho$*. Note that this factor,* ρ*, is inherent to and depending on the chosen modulation scheme. That is, we have*

$$\mathsf{Mod} : M \times \mathcal{R}_{>0} \to \Sigma^\rho, (\mu, s) \mapsto \left(\sigma_1, \ldots, \sigma_\rho\right). \tag{3}$$

Correspondingly, the demodulation function Demod *takes as input* ρ *signals* $\sigma_1, \ldots, \sigma_\rho$ *and outputs a message symbol* $\mu \in M$ *(or, in case that demodulation is not possible, it outputs* $\perp$*):*

$$\mathsf{Demod} : \Sigma^\rho \to M \cup \{\perp\},\ \left(\sigma_1, \ldots, \sigma_\rho\right) \mapsto \mu. \tag{4}$$

Demod *is the inverse function of* Mod *if the signal strength is sufficiently strong. That is, it holds for all* $\mu \in M$ *that*

$$\mathsf{Demod}(\mathsf{Mod}(\mu, s)) = \mu \tag{5}$$

if $s \geq \tau$ *for some threshold* τ*.*

Depending on the specific modulation scheme, not all signal parameters may influence the demodulation with regard to the extracted message, e. g., when using phase shift keying, the amplitude and frequency are only needed to identify the *signal*, but have no influence on the actual encoded *information* as this only depends on the observed phase shift compared to the underlying carrier frequency. A low amplitude, however, may prevent a receiver from successfully demodulating signals into messages.

3.2.3 Sending and Receiving Message Symbols

Sending a message symbol μ means to modulate it into a sequence $\sigma_1,\dots,\sigma_\rho$ of signals with respect to some signal strength s, using the Mod function, and to send these over one of the communication channels, by writing each signal σ_i on a comm-out tape. This procedure is formally captured by the Send operation.

Definition 4 (The Send Operation)**.** *The* Send *operation takes as input a triple* (CT,μ,s) *where* CT *is a comm-out tape of* $\mathcal{P}$*,* $\mu \in M$ *is a message symbol, and* $s \in \mathcal{R}_{>0}$ *represents a signal strength. It involves to execute first* $\mathsf{Mod}(\mu,s)$ *to get a sequence of* ρ *signals* $\sigma_1,\dots,\sigma_\rho$*. These are written step-by-step onto the tape* CT*. Note that* Send *does not specify the intended recipient of the message symbol* μ *but the communication channel. Recall that during one time slot, a party* $\mathcal{P}$ *can only write to the* t*-th cell. That is, the writing procedure is formally equivalent to setting* ρ *consecutive cells of* CT *as follows:*

$$\mathsf{CT}[t] := \sigma_1,\dots,\mathsf{CT}[t+\rho-1] := \sigma_\rho. \tag{6}$$

Therefore, the Send *operation influences the current and the next* $\rho-1$ *cells of the comm-out tape* CT*, which, in total, takes* ρ *time slots to perform.*

We extend the notation to the case of sending messages: for a message $m=(\mu_1,\dots,\mu_\ell)$*, we define by* $\mathsf{Send}(\mathsf{CT},m,s)$ *the sequence of operations* $\mathsf{Send}(\mathsf{CT},\mu_i,s)$*,* $i=1,\dots,\ell$*.*

Likewise, parties can *receive* message symbols from their comm-in tapes and only from these.

Definition 5 (The $\mathsf{Receive}$ Operation)**.** *The* $\mathsf{Receive}$ *operation takes as input a comm-in tape* CT*. It reads out the current* ρ *entries of* CT*, i. e.,* $\mathsf{CT}[t],\dots,\mathsf{CT}[t+\rho-1]$*. Given this,* $\mathsf{Demod}(\mathsf{CT}[t],\dots,\mathsf{CT}[t+\rho-1])$ *is executed to get a message symbol* $\mu \in M \cup \{\perp\}$*. Then,* μ *represents the output of* $\mathsf{Receive}$*.*

Since the Demod function requires ρ signals for extracting a message, and as there is no possibility to receive future signals in advance, this definition implies that $\mathsf{Receive}$ needs to wait for ρ time slots for returning a message μ, i.e., until the demodulation function received enough signals to return a message symbol $\mu \neq \perp$.

3.2.4 Signal Collision

As the parties may share the same physical channel, different signals might *collide*. Formally, this means that parallel writing on communication tapes is possible, in contrast to the MitMM. This and the fact that accessing communication cells "from the past" is not possible, imply that the WCM is not message-driven.

For two signals $\sigma,\sigma' \in \Sigma$, we denote by

$$\sigma+\sigma' \tag{7}$$

the resulting signal. That is, if two different signals σ and σ' are simultaneously received on the same tape CT, then $\sigma+\sigma'$ appears on the tape instead (see Sec. 3.3 for more details).

The concrete working of the collision depends on the underlying physical channel and the selected modulation/demodulation procedures.

Nonetheless, some properties hold in all cases. For instance, it holds that

$$\sigma+0 = 0+\sigma = \sigma \tag{8}$$

for all signals σ. Furthermore, collision is commutative and associative:

$$\sigma+\sigma' = \sigma'+\sigma \text{ and } \sigma+(\sigma'+\sigma'') = (\sigma+\sigma')+\sigma'' . \tag{9}$$

Collision is also commutative with respect to Shift, i. e.,

$$\mathsf{Shift}_\varphi(\sigma+\sigma') = \mathsf{Shift}_\varphi(\sigma)+\mathsf{Shift}_\varphi(\sigma') .$$

In some special cases, the signals amplify or annihilate each other, depending on their relative phase shift. More precisely, it holds

$$(A,f,\varphi)+(A',f,\varphi) = (A+A',f,\varphi) \tag{10}$$

$$(A,f,\varphi)+(A',f,\varphi+\pi) = \begin{cases}(A-A',f,\varphi), & \text{if } A \geq A' \\ (A'-A,f,\varphi+\pi), & \text{else.}\end{cases} \tag{11}$$

In particular, $(A,f,\varphi)+(A,f,\varphi+\pi)=0$. Consequently, we define for a given signal $\sigma=(A,f,\varphi)$ its inverse as

$$-\sigma := (A,f,\varphi+\pi) . \tag{12}$$

Channels are characterized by signals that share the same frequency f within a certain bandwidth. These are usually chosen such that the interference between different channels is as small as possible.[3] For these reasons, we focus on collisions of signals that occur on the same channel. Moreover, for a given frequency f, we use the term Σ_f to refer to the set

[3] For instance, in IEEE 802.15.4 the channels in the 2.4 GHz band are non-overlapping as they are 5 MHz apart with a bandwidth of 2 MHz (IEEE, 2011).

of signals that have f as frequency (approximately). That is, signals belong to the same channel if and only if they are elements of the same space Σ_f for a selected frequency f. It holds for any frequency f that

$$\sigma, \sigma' \in \Sigma_f \Rightarrow \sigma + \sigma' \in \Sigma_f \ . \tag{13}$$

Formally, this means that Σ_f is closed under $+$. Together with the properties mentioned above, it follows that $(\Sigma_f, +)$ forms a commutative group. This view is for example helpful when describing the effects of jamming, e. g., see Sec. 5.1.

3.3 Locality in the WCM

In wireless communication, signals are *physical* objects. This has a number of consequences that are not covered by the MitMM, e. g., multiple signals can collide, yielding different resulting signals (cf. Sec. 3.2.4). Further relevant aspects are:

1. Once a party sends a signal, it takes *time* until it reaches another party.
2. During transmission, the signal strength may *decrease*.

To represent these aspects, we adopt and extend the notion of being linked (cf. (Katz, 2002, Definition 2.2)). Due to the fact that all parties rely on *public* physical channels, any two parties are linked in the sense that, potentially, messages can be exchanged. Here, we also have to take into account their relative locations. To this end, we propose the following formal definition of linkage:

Definition 6 (Linkage between two parties)**.** *Consider two parties $\mathcal{P}, \mathcal{P}' \in \Pi \cup \{\mathcal{A}\}$ with $\mathcal{P} \neq \mathcal{P}'$. The* linkage *from $\mathcal{P}$* to *$\mathcal{P}'$, denoted by $\mathsf{Link}(\mathcal{P}, \mathcal{P}')$, is defined by a tuple*

$$\mathsf{Link}(\mathcal{P}, \mathcal{P}') = (\delta; \lambda_1, \ldots, \lambda_{\mathsf{chs}}) \tag{14}$$

where

- *$\delta \in \mathbb{N}_{\geq 0}$ is a non-negative integer, representing the time delay, and*
- *$\lambda_i : \Sigma \to \Sigma$ is a probabilistic procedure, dubbed linkage procedure, that expresses how a signal sent by $\mathcal{P}$ (using the i-th comm-out tape) arrives at $\mathcal{P}'$ on the i-th comm-in tape.*

The linkage between two parties expresses when and what kind of signal arrives at $\mathcal{P}'$ if $\mathcal{P}$ sends some signal. As an example, the expected path loss due to the distance between sender and recipient could be expressed by $\lambda_i(A, f, \varphi) = (A', f, \varphi)$ with $A' < A$.

Another example is a channel-induced phase shift on transmitted signals. Assume that $\mathcal{P}$ and $\mathcal{P}'$ have a *physical* distance d to each other which has the form $d = \delta \cdot \frac{c}{f_i} + r = \delta \cdot \frac{c}{f_i} + \varphi_i \cdot \frac{c}{2\pi f_i}$, with an integer $\delta \geq 0$, the speed of light constant c, the i-th communication channel's carrier frequency f_i, and the remainder r with $0 \leq r < \frac{c}{f_i}$. That is, d is *not* a multiple of the carrier frequency's wavelength. Then, $\lambda_i(A, f, \varphi) = (A', f', \varphi + 2\pi - \varphi_i) = (A', f', \varphi')$.

Recall that we have one linkage procedure λ_i per channel with a total of chs available channels and a fixed order (cf. Sec. 3.1). Now, assume that some party $\mathcal{P}$ writes a signal σ on one of its comm-out tapes $(\mathsf{CT}_{\text{out}})_i^{\mathcal{P}}$, i. e., $(\mathsf{CT}_{\text{out}})_i^{\mathcal{P}}[t] := \sigma$. Writing on CT automatically affects *all* comm-in tapes of parties that are linked to $\mathcal{P}$. That is, let $\mathcal{P}' \neq \mathcal{P}$ be some other party and let $\mathsf{Link}(\mathcal{P}, \mathcal{P}') = (\delta; \lambda_1, \ldots, \lambda_{\mathsf{chs}})$ be the linkage between $\mathcal{P}$ and $\mathcal{P}'$. The procedure of $\mathcal{P}$ writing σ into the cell $(\mathsf{CT}_{\text{out}})_i^{\mathcal{P}}[t]$ impacts the content of the corresponding comm-in tape $(\mathsf{CT}_{\text{in}})_i^{\mathcal{P}'}$ for party $\mathcal{P}' \neq \mathcal{P}$ as follows:

$$(\mathsf{CT}_{\text{in}})_i^{\mathcal{P}'}[t+\delta] := \lambda_i(\sigma) \ + \ (\mathsf{CT}_{\text{in}})_i^{\mathcal{P}'}[t+\delta] \ . \tag{15}$$

That is, the signal which is already existing on $(\mathsf{CT}_{\text{in}})_i^{\mathcal{P}'}$, expressed by $(\mathsf{CT}_{\text{in}})_i^{\mathcal{P}'}[t+\delta]$, is updated to $\lambda_i(\sigma) \ + \ (\mathsf{CT}_{\text{in}})_i^{\mathcal{P}'}[t+\delta]$. This definition allows to cover the aspects mentioned above:

1. When party $\mathcal{P}$ sends a signal σ at some point in time t, σ reaches $\mathcal{P}'$ only with some time delay δ. That is, $\mathcal{P}$ writes on cell $(\mathsf{CT}_{\text{out}})_i^{\mathcal{P}}[t]$, i. e., with index t, but this affects $(\mathsf{CT}_{\text{in}})_i^{\mathcal{P}'}[t+\delta]$, i. e., δ time slots later.
2. σ physically traverses the space between $\mathcal{P}$ and $\mathcal{P}'$ and arrives as $\lambda_i(\sigma)$ at $\mathcal{P}'$.
3. If there is already a signal present on the tape's targeted cell $(\mathsf{CT}_{\text{in}})_i^{\mathcal{P}'}[t+\delta]$, then it collides with $\lambda_i(\sigma)$ (cf. Eq. (15)).

A schematic overview is depicted in Fig. 1.

Finally, we introduce two notions with respect to the time delay:

Definition 7 (Time Delay Symmetry and Triangle Inequality)**.** *Consider a set of parties Π and their linkages $\mathsf{Link}(\mathcal{P}, \mathcal{P}')$ for any $\mathcal{P} \neq \mathcal{P}' \in \Pi$. We denote by $\delta_{\mathcal{P},\mathcal{P}'}$ the time delay in $\mathsf{Link}(\mathcal{P}, \mathcal{P}')$.*

We say that the time delay parameter is symmetric with respect to these linkages if it holds for any $\mathcal{P} \neq \mathcal{P}' \in \Pi$ that

$$\delta_{\mathcal{P},\mathcal{P}'} = \delta_{\mathcal{P}',\mathcal{P}}. \tag{16}$$

Moreover, we say that the time delay parameter fulfills the triangle inequality if it holds for any pairwise distinct $\mathcal{P}, \mathcal{P}', \mathcal{P}'' \in \Pi$ that

$$\delta_{\mathcal{P},\mathcal{P}''} \leq \delta_{\mathcal{P},\mathcal{P}'} + \delta_{\mathcal{P}',\mathcal{P}''}. \tag{17}$$

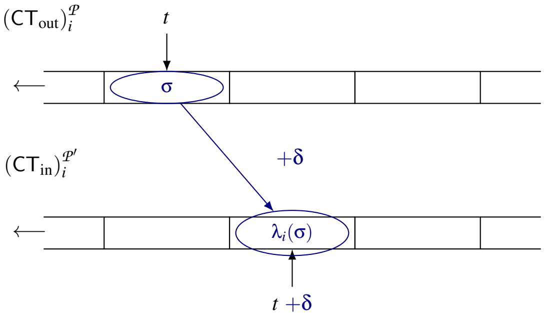
$(\mathsf{CT}_{\mathrm{out}})_i^{\mathcal{P}}$
t
σ
$+\delta$
$(\mathsf{CT}_{\mathrm{in}})_i^{\mathcal{P}'}$
$\lambda_i(\sigma)$
$t+\delta$

Figure 1: Linkage from $(\mathsf{CT}_{\mathrm{out}})_i^{\mathcal{P}}$ to $(\mathsf{CT}_{\mathrm{in}})_i^{\mathcal{P}'}$ with delay δ.

If not stated otherwise, in the following, we assume that the delays of the different linkages are symmetric and fulfill the triangle inequality.[4]

4 WIRELESS ATTACKER MODEL

Recall that in the MitMM, an attacker is mainly characterized by her ability to stop, forward, and modify messages at her wish. In the following, we discuss if and to what extent this is still given in the WCM. To this end, we introduce the Wireless Attacker Model (WAM). In Sec. 4.1, we explain an attacker's alleged capabilities. Based on this, we investigate the possibilities for jamming (tampering with) signals in Sec. 4.2.

4.1 Capabilities

Analogous to the MitMM, for the WAM, we consider an attacker who is completely characterized by her abilities to access her communication tapes. This means she can send signals by writing to her comm-out tapes and receive signals by reading from her comm-in tapes. Furthermore, the attacker is non-invasive in the sense that she does *not* tamper with the parties or the environment, but only sends or receives signals. However, an attacker is not restricted in her choice of signals. That is, the signals do not need to be related to the modulation of a message symbol. Of course, she may still choose to use Mod and Send functions for communicating.

Moreover, we assume that the attacker has full knowledge about the communication channels between her and other parties. Formally, thus, the attacker $\mathcal{A}$ knows $\mathsf{Link}(\mathcal{A},\mathcal{P})$ and $\mathsf{Link}(\mathcal{P},\mathcal{A})$ for all $\mathcal{P} \in \Pi$. On the other hand, linkages between any two parties $\mathcal{P},\mathcal{P}' \in \Pi$ *not* involving the attacker are only partially known to her. As motivated in Sec. 2.4.2, $\mathcal{A}$ only knows the respective delay parameter δ of $\mathsf{Link}(\mathcal{P},\mathcal{P}')$, while the λ_i remain secret.

4.2 Jamming (Modification) of Signals

In the field of wireless communication, jamming refers to any intentional interference with signals and possible modifications thereof. Hence, we use *jamming* to express any change of the signal incurred by an attacker. One important difference between tampering in the MitMM and jamming in the WCM is that, in the latter, messages are composed of message symbols which are modulated into a sequence of ρ signals. Thus, whether the alteration of signals results in any changes in the message received by $\mathcal{P}'$ depends at least on the demodulation procedure Demod and how the semantic message is derived from the message symbols. For example, a flip of a single bit might render a message unreadable if this change violates some checksum or have no effect if some error correction codes are used. So, we focus only on if and how an attacker may change *signals* and leave the discussion on the impact on messages to the individual scenarios.

For the discussion on jamming signals, consider two parties $\mathcal{P},\mathcal{P}'$. At time t, $\mathcal{P}$ sends a signal σ to $\mathcal{P}'$, i. e., writes σ on one of its comm-out tapes $(\mathsf{CT}_{\mathrm{out}})_i^{\mathcal{P}}$. Let the linkage between $\mathcal{P}$ and $\mathcal{P}'$ be denoted by $\mathsf{Link}(\mathcal{P},\mathcal{P}') = \left(\delta_{\mathcal{P},\mathcal{P}'};\lambda_1,\ldots,\lambda_{\mathsf{chs}}\right)$. If no other signals are present on the same channel, then,

$$(\mathsf{CT}_{\mathrm{in}})_i^{\mathcal{P}'}[t+\delta_{\mathcal{P},\mathcal{P}'}] = \lambda_i\left((\mathsf{CT}_{\mathrm{out}})_i^{\mathcal{P}}[t]\right) \qquad (18)$$

represents the signal received by $\mathcal{P}'$.

For $\mathcal{A}$, the only option to influence σ is to send her own signal such that it collides with the signal received by $\mathcal{P}'$. Let $\mathsf{Link}(\mathcal{A},\mathcal{P}') = \left(\delta_{\mathcal{A},\mathcal{P}'};\lambda_1^*,\ldots,\lambda_{\mathsf{chs}}^*\right)$ be the linkage between $\mathcal{A}$ and $\mathcal{P}'$. Then, jamming means to achieve a collision $(\mathsf{CT}_{\mathrm{in}})_i^{\mathcal{P}'}[t+\delta_{\mathcal{P},\mathcal{P}'}] = \sigma + \sigma^*$ with $\sigma = \lambda_i\left((\mathsf{CT}_{\mathrm{out}})_i^{\mathcal{P}}[t]\right)$ and $\sigma^* = \lambda_i^*\left((\mathsf{CT}_{\mathrm{out}})_i^{\mathcal{A}}[t+\delta_{\mathcal{P},\mathcal{P}'}-\delta_{\mathcal{A},\mathcal{P}'}]\right)$. Hence, $\mathcal{A}$ has to write a signal on her comm-out tape no later than $t+\delta_{\mathcal{P},\mathcal{P}'}-\delta_{\mathcal{A},\mathcal{P}'}$. Obviously, if $\delta_{\mathcal{P},\mathcal{P}'} < \delta_{\mathcal{A},\mathcal{P}'}$, i. e., the distance between $\mathcal{P}$ and $\mathcal{P}'$ is smaller than the distance between $\mathcal{P}'$ and $\mathcal{A}$, an attacker would have to send her signal even *before* $\mathcal{P}$ sent σ. In certain cases, this may be possible — for instance, if σ is part of a longer message and $\mathcal{A}$ can anticipate that σ (or some signal) will be sent. Still, in such cases, $\mathcal{A}$ cannot *react* to signals from $\mathcal{P}$. The same holds if $\delta_{\mathcal{P},\mathcal{P}'} < \delta_{\mathcal{P},\mathcal{A}}$. Here, σ from $\mathcal{P}$, i. e., the signal that $\mathcal{A}$ aims to jam, would reach $\mathcal{P}$' *before* it reaches $\mathcal{A}$.

[4] In fact, we cannot think of any contradictory practical scenario.

Besides sending the jamming signal in time, another challenge is to pick and send a signal that effectively jams. Recall that, in some special cases, two signals can amplify or annihilate each other (cf. Sec. 3.2.4). An amplified signal, however, does not necessarily affect a modulated message. That is, the effectiveness of a jamming signal strongly depends on the chosen modulation.

Summing up, to manipulate signals received by other parties, a wireless attacker has to decide *when* and *what* signals she sends. Depending on her jamming strategy, e. g., constant or reactive jamming, this can be less or more challenging.[5]

5 APPLICATIONS

To demonstrate the applicability of the proposed model, in this section, we revisit friendly jamming which cannot be represented in the MitMM, and we explain how the WCM and WAM can be used for analysis. We also shortly discuss how Distance Bounding protocols and Frequency-Hopping Spread Spectrum can be modelled, but omit the details here to conserve space. Note that each of the different components listed in Sec. 2 are required at least once, showing that at least these three are required for a comprehensive wireless communication model.

5.1 Friendly Jamming for Confidentiality

Complementing the usually destructive jamming (cf. Sec. 4.2), so-called *friendly jamming* (e. g., (Jin et al., 2022; Jin et al., 2021; Jeon et al., 2022; Shen et al., 2013; Berger et al., 2016; Berger et al., 2014; Li et al., 2022; Li et al., 2020)) approaches turn the tables and use deliberate jamming as a defensive measure. This way, jamming is used to block unauthorized messages (*authorization*) or to hide the content of communication from illegitimate parties (*confidentiality*).

An example is the protection of communication to and from an Implantable Medical Device (IMD) which is only capable of plain (unencrypted) communication as presented by (Gollakota et al., 2011). They propose an external device, the *shield*, which is worn on the body near an IMD acting as a gateway. Using a two-radio design, the shield utilizes friendly jamming to enforce authorization and confidentiality concerning the communication with the IMD. Due to its design, the shield is capable of reconstructing the original data signals, while any other party only receives jammed signals. However, (Gollakota et al., 2011) do not provide any formal representation of the security goals and analysis in their work.

5.1.1 Formalization of Friendly Jamming

The typical scenario of friendly jamming considers two collaborating parties, the jamming party J and the receiving party R. These two have an additional private communication channel (cf. Sec. 3.1). The overall goal of friendly jamming is to protect a signal σ. For example, in the use case of (Gollakota et al., 2011), σ could either be a signal coming from the IMD to hide its content or be a non-genuine signal going to the IMD to render it illegible. To this end, J generates a jamming signal γ and sends it such that it collides with σ. As a consequence, a potential attacker only sees $\sigma+\gamma$. To reverse the jamming, J shares with R all information necessary such that R can create an appropriate antidote signal α. Colliding α with $\sigma+\gamma$ yields σ again.

Note that this approach requires J to send γ in time, which can be challenging in practice (cf. Sec. 4.2). As this depends on various aspects such as the relative positions of parties, the reaction time of J, etc., we consider this as a separate question and focus on the generation of the jamming signal and its antidote. Consequently, one can formalize such a scheme as follows:

Definition 8 (Friendly Jamming Scheme). [6] *A friendly jamming scheme* $(\mathsf{Gen}, \mathsf{Jam}, \mathsf{Antijam}, \Sigma_f)$ *is composed of three algorithms and a signal space restricted to some frequency* f. $\mathsf{Gen}(\chi)$ *takes as input a security parameter* χ *and outputs a seed* κ. $\mathsf{Jam}(\kappa)$ *takes as input some seed* κ *and creates a jamming signal* $\gamma \in \Sigma_f$. $\mathsf{Antijam}(\kappa)$ *takes as input some seed* κ *and creates an antidote signal* $\alpha \in \Sigma_f$.

The scheme is correct if for all security parameters χ *and for all seeds* $\kappa \leftarrow \mathsf{Gen}(\chi)$*, it holds that*

$$\mathsf{Jam}(\kappa) + \mathsf{Antijam}(\kappa) = 0\,. \tag{19}$$

Correctness essentially means that $\mathsf{Antijam}(\kappa) = -\mathsf{Jam}(\kappa)$ for all seeds (cf. Sec. 3.2.4). Besides correctness, a friendly jamming scheme should also be sound. Depending on the application, different security goals may be considered, e. g., authenticity, or confidentiality. In the following, we focus on confidentiality.

Intuitively, confidentiality means that one cannot reconstruct the original message from the jammed

[5] For details on different jamming strategies, we refer to (Xu et al., 2005; Grover et al., 2014).

[6] For the sake of simplicity, here, we consider one signal only. The formalization can be extended easily to a sequence of signals.

signals. To formalize this security goal, we adopt the established security definition of $\mathsf{IND\text{-}CPA}$ (Indistinguishability under Chosen Plaintext Attack) and introduce $\mathsf{IND\text{-}CSA}\text{-}n$ (Indistinguishability under Chosen Signal Attack). The parameter n indicates the main difference to $\mathsf{IND\text{-}CPA}$: an attacker could be using n antennas, formally represented by n parties under the attacker's control.

Definition 9 ($\mathsf{IND\text{-}CSA}\text{-}n$ Game)**.** *The $\mathsf{IND\text{-}CSA}\text{-}n$ game with respect to some friendly jamming scheme $(\mathsf{Gen}, \mathsf{Jam}, \mathsf{Antijam}, \Sigma_f)$ considers an oracle $\mathcal{O} = \{\mathcal{O}_1, \mathcal{O}_2\}$ and an attacker $\mathcal{A} = \{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$. Each oracle has access to one comm-out tape and each attacker to one comm-in tape. The tapes controlled by $\mathcal{O}$ are linked to all tapes controlled by $\mathcal{A}$. For $i \in \{1,2\}$ and $j \in \{1,\ldots,n\}$, we denote by $\lambda_{i,j}$ the linkage procedure of the linkage between the comm-out tape of $\mathcal{O}_i$ and the comm-in tape of $\mathcal{A}_j$.*

$\mathcal{A}$ chooses two signals $\sigma_0 \neq \sigma_1 \in \Sigma_f$ and sends these to $\mathcal{O}$. Then, $\mathcal{O}$ generates a (secret) seed $\kappa \leftarrow \mathsf{Gen}(\chi)$ and jamming signal $\gamma \leftarrow \mathsf{Jam}(\kappa)$. It samples uniformly $b \xleftarrow{\$} \{0,1\}$ and, at time t, instructs $\mathcal{O}_1$ to write σ_b on $(\mathsf{CT}_{\mathrm{out}})^{\mathcal{O}_1}$ and $\mathcal{O}_2$ to write γ on $(\mathsf{CT}_{\mathrm{out}})^{\mathcal{O}_2}$ (simultaneously). Consequently, $\mathcal{A}_j$ receives the collided signal

$$\sigma_j^{col} = \lambda_{1,j}(\sigma_b) + \lambda_{2,j}(\gamma)\,. \tag{20}$$

$\mathcal{A}$ outputs $b^* \in \{0,1\}$ and wins if $b^* = b$. A friendly jamming scheme is called $\mathsf{IND\text{-}CSA}\text{-}n$-secure with respect to the linkage procedures $\{\lambda_{i,j}\}_{i=1,2;j=1,\ldots,n}$ if the attacker's advantage $\mathsf{Adv}(\mathcal{A}) = \left|\Pr[\mathcal{A}\ wins] - \frac{1}{2}\right|$ is negligible in χ.

5.1.2 $\mathsf{IND\text{-}CSA}\text{-}2$ Attacker

Given the formalization, the logical next step is to ask if $\mathsf{IND\text{-}CSA}\text{-}n$ security can be achieved for any realistic choice of $\{\lambda_{i,j}\}$. While this might be possible for the $\mathsf{IND\text{-}CSA}\text{-}1$ case, (Tippenhauer et al., 2013) describe an $\mathsf{IND\text{-}CSA}\text{-}2$ attacker. In the following, we use the notation from Def. 9 with $n = 2$ to describe this attack. The attack assumes a set of linkage procedures $\{\lambda_{1,1}, \lambda_{1,2}, \lambda_{2,1}, \lambda_{2,2}\}$ such that

$$\lambda_{1,1} = \lambda_{2,2} = \mathrm{id} \quad \text{and} \quad \lambda_{1,2} = \lambda_{2,1} = \mathsf{Shift}_{\frac{\pi}{2}}\,. \tag{21}$$

(Tippenhauer et al., 2013) demonstrates that this can be possible in practice if the locations for $\mathcal{A}_1$ and $\mathcal{A}_2$ are chosen such that the four parties $\mathcal{O}_1, \mathcal{O}_2, \mathcal{A}_1, \mathcal{A}_2$ form an isosceles trapezoid, while the following properties must be satisfied:

1. The distance d between $\mathcal{O}_1$ and $\mathcal{O}_2$ is smaller than half of the carrier frequency's wavelength, while the distance between $\mathcal{A}_1$ and $\mathcal{A}_2$ is greater than half this wavelength (and d).
2. The delays between $\mathcal{O}_1$ and $\mathcal{A}_1$, and between $\mathcal{O}_2$ and $\mathcal{A}_2$, respectively, are equal. Likewise, the delays between $\mathcal{O}_2$ and $\mathcal{A}_1$, and between $\mathcal{O}_1$ and $\mathcal{A}_2$, respectively, are also equal.
3. $\mathcal{A}_2$ (or $\mathcal{A}_1$) perceives signals from $\mathcal{O}_1$ (or $\mathcal{O}_2$) with a channel-induced phase shift of $\frac{\pi}{2}$ relative to $\mathcal{A}_1$ (or $\mathcal{A}_2$).

Due to the differing phase offsets (cf. Eq. (21)), the signals received by $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively, are

$$\sigma_1^{\mathrm{col}} = \lambda_{1,1}(\sigma) + \lambda_{2,1}(\gamma) = \sigma + \mathsf{Shift}_{\frac{\pi}{2}}(\gamma)$$
$$\sigma_2^{\mathrm{col}} = \lambda_{1,2}(\sigma) + \lambda_{2,2}(\gamma) = \mathsf{Shift}_{\frac{\pi}{2}}(\sigma) + \gamma\,.$$

The attacker shifts and collides these two signals as follows:

$$\begin{aligned}&\mathsf{Shift}_{\frac{3\pi}{2}}(\sigma_1^{\mathrm{col}}) + \mathsf{Shift}_{\pi}(\sigma_2^{\mathrm{col}}) \\ &= \mathsf{Shift}_{\frac{3\pi}{2}}(\sigma) + \mathsf{Shift}_{2\pi}(\gamma) + \mathsf{Shift}_{\frac{3\pi}{2}}(\sigma) + \mathsf{Shift}_{\pi}(\gamma) \\ &= \mathsf{Shift}_{\frac{3\pi}{2}}(\sigma) + \mathsf{Shift}_{\frac{3\pi}{2}}(\sigma)\,.\end{aligned}$$

That is, the attacker reconstructed an amplified variant of σ, which immediately allows to reconstruct σ.

5.2 Distance Bounding Protocols

Distance Bounding (DB) protocols were introduced by Brands and Chaum (Brands and Chaum, 1994). Their purpose is for a prover P to authenticate himself to a verifier V and to demonstrate his proximity to V. To this end, the verifier measures the round trip time and, based on the propagation speed of electromagnetic waves, calculates an upper bound to the distance, such that the verifier is convinced that the prover cannot be further away than this calculated bound.

In our model, the timing aspect can be captured by the delay parameter δ in the linkage between two parties (cf. Def. 6). More concretely, consider the two parties $\mathcal{P}, \mathcal{P}'$ where $\mathcal{P}$ wants to determine the distance to $\mathcal{P}'$. Moreover, assume the linkages $\mathsf{Link}(\mathcal{P}, \mathcal{P}')$ and $\mathsf{Link}(\mathcal{P}', \mathcal{P})$ with a symmetric delay δ (cf. Def. 7). Then, the round trip time between $\mathcal{P}$ and $\mathcal{P}'$ is at least $2 \cdot \delta$. Thus, measuring the round trip time gives a lower bound on δ which in turn gives an upper bound on the *geographical* distance between them.

5.3 Frequency-Hopping Spread Spectrum

The basic idea of the Frequency-Hopping Spread Spectrum (FHSS) technique is to not stick to one physical channel during communication but to hop across available channels (pseudo-)randomly. This provides more robustness against interference on a specific frequency and, at the same time, makes it harder for an attacker to target the correct channel if the hop sequence is secret. Our model naturally offers to incorporate FHSS by switching between different communication tapes when sending messages, whereas tapes essentially represent different channels with different carrier frequencies.

We illustrate this for a variant of FHSS where the messages sent by $\mathcal{P}$ are indexed, i. e., $m_1, m_2, \ldots$, and where, for each message, the communication channel is separately chosen. To this end, sender $\mathcal{P}$ and receiver $\mathcal{P}'$ agree on a secret key k to initialize a pseudorandom function $f_k : \mathbb{N} \rightarrow \{1, \ldots, \mathsf{chs}\}$. For each message m_i, f_k determines which communication tape is to be chosen. More precisely, sending the i-th message means that $\mathcal{P}$ executes

$$\mathsf{Send}((\mathsf{CT}_{\mathrm{out}})^{\mathcal{P}}_{f_k(i)}, m_i, s) \ . \tag{22}$$

Likewise, $\mathcal{P}'$ uses f_k to determine the channel to listen to next.

6 RELATED WORK AND CONCLUSION

While several works discuss possible extensions of the Dolev-Yao model, e. g., see (Mao, 2004; Herzog, 2005), we focus on these that address the connection of the MitMM and wireless attackers.

(Pöpper et al., 2011) question the applicability of the MitMM in the context of wireless communication. They show the difficulties of symbol flipping and signal annihilation and that these succeed with a certain probability only. In contrast to our work, the proposal of an appropriate model is out of scope.

(Schaller et al., 2009) (see also (Basin et al., 2009; Basin et al., 2011)) developed a formal model for wireless networks concerning physical properties in the form of inductive, trace-based, symbolic approaches for use with a theorem prover. In fact, some of the aspects identified for the WCM are also reflected there, e. g., the properties of communication (transmission delays based on distance and propagation speed), location (of network nodes), and time (for temporal dependencies). However, there are also numerous differences. For example, messages are sent in the form of events, transmission time is independent of the message length. Modulation schemes, the resulting signals, and different available communication channels are not considered. This means that schemes like FHSS and (Gollakota et al., 2011) (Sec. 5.1) cannot be fully represented by their model.

(Rocchetto and Tippenhauer, 2016) proposed CPDY, an extended Dolev-Yao model for cyber-physical systems, to allow for covering physical interactions between components and the notion of distance. However, they propose and implement new rules in a formal security specification language while focusing on physical interactions in the literal sense, e. g., an attacker physically manipulates a device, while our focus lies on the communication between parties.

(Avoine et al., 2021) review relay attacks and the threat model of DB protocols in general. They also consider effects existing in practice, e. g., provers' processing delays, and relate these with theoretical approaches to proving security for DB protocols. They conclude that formal models for DB protocols are inaccurate as these make impractical assumptions, e. g., processing delays during the fast phase are assumed to be non-existent, or colluding attackers are disallowed to communicate during the fast phase. However, they do this without proposing any formal model.

We share the view of (Avoine et al., 2021) that more realistic models are necessary. Our model imposes no further restrictions on the communication between colluding attackers or other parties, neither during the fast phase nor any other. The only requirement is that any (wireless) communication has to follow the physical rules laid out by our model, e. g., signal properties and delays are still in effect. As our model is focused on the communication between parties, processing delays are not present in our model either.

(Dürholz et al., 2011) provide a formal (simulator-assisted) analysis of DB Radio-Frequency Identification (RFID) protocols. They propose formal models for Mafia, terrorist, and distance fraud, which they apply on the RFID DB scheme by (Kim and Avoine, 2009) as an example. While Dürholz et al. also consider a global clock, their concept of time is message-driven, i. e., a unit of time represents a complete protocol message and is thus independent of the message's length. On the one hand, they consider noisy communication based on the constraints for RFID and wireless communication, on the other hand, modulation schemes, signals, and channels seem irrelevant for the RFID scenario.

(Boureanu et al., 2021) developed a parameterized cryptographic model for DB. Finally, they point out possible attacks on existing DB schemes and implement their (parameterized) model in an interactive cryptographic prover which they apply on a contactless payment scheme to prove Man-in-the-Middle security. In their model, Boureanu et al. define notions of time, location, and distances, additionally, they define oracles to capture an attacker's capabilities. Also, the provided oracles bear some similarity to our defined operations. However, modulation schemes, signal properties, and available channels remain unconsidered. Furthermore, the provided `replace` oracle allows for targeted replacing of select message bits for an arbitrary subset of parties *independent* of their relative positions, thereby ignoring the fact that different parties may receive message bits at different times based on their positions. Note that, in our model, an attacker needs to actively send signals that overlap with the original signals (as this is the only possibility to influence a received signal) and that she cannot influence the time at which the original signals reach the receivers.

Our proposed cryptographic model allows to represent existing mechanisms that build on the peculiarities of wireless communication. We presented existing schemes that can only be represented using the three aspects identified in Sec. 2, i. e., communication channels, signals, and locality. We hope that our model will be useful for further analysis and design of cryptographic schemes in the wireless area.

ACKNOWLEDGEMENTS

This research was supported by the project *Physical Guards* funded by the Federal Ministry for Education and Research of Germany (BMBF).

REFERENCES

Avoine, G., Boureanu, I., Gérault, D., Hancke, G. P., Lafourcade, P., and Onete, C. (2021). From relay attacks to distance-bounding protocols. In Avoine, G. and Hernandez-Castro, J., editors, *Security of Ubiquitous Computing Systems: Selected Topics*, pages 113–130. Springer International Publishing, Cham.

Basin, D., Capkun, S., Schaller, P., and Schmidt, B. (2009). Let's get physical: Models and methods for real-world security protocols. In Berghofer, S., Nipkow, T., Urban, C., and Wenzel, M., editors, *Theorem Proving in Higher Order Logics*, pages 1–22, Berlin, Heidelberg. Springer Berlin Heidelberg.

Basin, D., Capkun, S., Schaller, P., and Schmidt, B. (2011). Formal reasoning about physical properties of security protocols. *ACM Trans. Inf. Syst. Secur.*, 14(2).

Berger, D. S., Gringoli, F., Facchi, N., Martinovic, I., and Schmitt, J. (2014). Gaining Insight on Friendly Jamming in a Real-World IEEE 802.11 Network. In *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks*, WiSec '14, pages 105–116, New York, NY, USA. Association for Computing Machinery.

Berger, D. S., Gringoli, F., Facchi, N., Martinovic, I., and Schmitt, J. B. (2016). Friendly jamming on access points: Analysis and real-world measurements. *IEEE Transactions on Wireless Communications*, 15(9):6189–6202.

Bluetooth SIG (2016). Bluetooth core specification. Version 5.0.

Boureanu, I., Drăgan, C. C., Dupressoir, F., Gérault, D., and Lafourcade, P. (2021). Mechanised Models and Proofs for Distance-Bounding. In *2021 IEEE 34th Computer Security Foundations Symposium (CSF)*, pages 1–16.

Boureanu, I., Mitrokotsa, A., and Vaudenay, S. (2015). Practical and Provably Secure Distance-Bounding. In Desmedt, Y., editor, *Information Security*, pages 248–258, Cham. Springer International Publishing.

Brands, S. and Chaum, D. (1994). Distance-bounding protocols. In Helleseth, T., editor, *Advances in Cryptology — EUROCRYPT '93: Workshop on the Theory and Application of Cryptographic Techniques Lofthus, Norway, May 23–27, 1993 Proceedings*, pages 344–359. Springer Berlin Heidelberg, Berlin, Heidelberg.

Desmedt, Y., Goutier, C., and Bengio, S. (1988). Special uses and abuses of the Fiat-Shamir passport protocol (extended abstract). In Pomerance, C., editor, *Advances in Cryptology — CRYPTO '87: Proceedings*, pages 21–39. Springer Berlin Heidelberg, Berlin, Heidelberg.

Dolev, D. and Yao, A. C. (1983). On the security of public key protocols. *IEEE Trans. Information Theory*, 29(2):198–207.

Drimer, S. and Murdoch, S. J. (2007). Keep your enemies close: Distance bounding against smartcard relay attacks. In *16th USENIX Security Symposium (USENIX Security 07)*, Boston, MA. USENIX Association.

Dürholz, U., Fischlin, M., Kasper, M., and Onete, C. (2011). A Formal Approach to Distance-Bounding RFID Protocols. In Lai, X., Zhou, J., and Li, H., editors, *Information Security*, pages 47–62, Berlin, Heidelberg. Springer Berlin Heidelberg.

Eberz, S., Strohmeier, M., Wilhelm, M., and Martinovic, I. (2012). A Practical Man-In-The-Middle Attack on Signal-Based Key Generation Protocols. In Foresti, S., Yung, M., and Martinelli, F., editors, *Computer Security – ESORICS 2012: 17th European Symposium on Research in Computer Security, Pisa, Italy, September 10-12, 2012. Proceedings*, pages 235–252. Springer Berlin Heidelberg, Berlin, Heidelberg.

Elbert, B. R. (2008). *Introduction to Satellite Communication*. The Artech House Telecommunications Library. Artech House, Inc, Boston, 3rd edition.

Gollakota, S., Hassanieh, H., Ransford, B., Katabi, D., and Fu, K. (2011). They can hear your heartbeats: Non-invasive security for implantable medical devices. In *Proceedings of the ACM SIGCOMM 2011 Conference*, SIGCOMM '11, pages 2–13. ACM.

Grover, K., Lim, A., and Yang, Q. (2014). Jamming and anti-jamming techniques in wireless networks: A survey. *Int. J. Ad Hoc Ubiquitous Comput.*, 17(4):197–215.

Hancke, G. P. and Kuhn, M. G. (2005). An RFID distance bounding protocol. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*, pages 67–73. IEEE.

Hershey, J., Hassan, A., and Yarlagadda, R. (1995). Unconventional cryptographic keying variable management. *IEEE Transactions on Communications*, 43(1):3–6.

Herzog, J. (2005). A computational interpretation of Dolev-Yao adversaries. *Theoretical Computer Science*, 340(1):57–81. Theoretical Foundations of Security Analysis and Design II.

IEEE (1997). 802.11-1997 - IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11-1997*, pages 1–445.

IEEE (2011). IEEE Standard for Local and metropolitan area networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs). *IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006)*, pages 1–314.

Jeon, G.-H., Lee, J.-H., Sung, Y.-S., Park, H.-J., Lee, Y.-J., Yun, S.-W., and Lee, I.-G. (2022). Cooperative friendly jamming techniques for drone-based mobile secure zone. *Sensors*, 22(3).

Jin, R., Zeng, K., and Jiang, C. (2022). Friendly spectrum jamming against mimo eavesdropping. *Wireless Networks*, 28(6):2437–2453.

Jin, R., Zeng, K., and Zhang, K. (2021). A reassessment on friendly jamming efficiency. *IEEE Transactions on Mobile Computing*, 20(1):32–47.

Katz, J. (2002). *Efficient Cryptographic Protocols Preventing "Man-in-the-Middle" Attacks*. PhD thesis, Columbia University.

Kim, C. H. and Avoine, G. (2009). Rfid distance bounding protocol with mixed challenges to prevent relay attacks. In Garay, J. A., Miyaji, A., and Otsuka, A., editors, *Cryptology and Network Security*, pages 119–133, Berlin, Heidelberg. Springer Berlin Heidelberg.

Li, J., Lei, X., Diamantoulakis, P. D., Fan, L., and Karagiannidis, G. K. (2022). Security optimization of cooperative noma networks with friendly jamming. *IEEE Transactions on Vehicular Technology*, 71(12):13422–13428.

Li, X., Dai, H.-N., Wang, Q., Imran, M., Li, D., and Imran, M. A. (2020). Securing internet of medical things with friendly-jamming schemes. *Computer Communications*, 160:431–442.

Mao, W. (2004). A structured operational modelling of the Dolev-Yao threat model. In Christianson, B., Crispo, B., Malcolm, J. A., and Roe, M., editors, *Security Protocols*, pages 34–46, Berlin, Heidelberg. Springer Berlin Heidelberg.

Mohammad Hasan (2022). State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally.

Pöpper, C., Tippenhauer, N. O., Danev, B., and Capkun, S. (2011). Investigation of Signal and Message Manipulations on the Wireless Channel. In Atluri, V. and Diaz, C., editors, *Computer Security – ESORICS 2011*, volume 6879 of *Lecture Notes in Computer Science*, pages 40–59. Springer-Verlag Berlin Heidelberg, Berlin, Heidelberg.

Ranganathan, A., Tippenhauer, N. O., Škorić, B., Singelée, D., and Čapkun, S. (2012). Design and implementation of a terrorist fraud resilient distance bounding system. In Foresti, S., Yung, M., and Martinelli, F., editors, *Computer Security – ESORICS 2012: 17th European Symposium on Research in Computer Security, Pisa, Italy, September 10-12, 2012. Proceedings*, pages 415–432. Springer Berlin Heidelberg, Berlin, Heidelberg.

Rasmussen, K. B. and Capkun, S. (2010). Realization of RF distance bounding. In *19th USENIX Security Symposium (USENIX Security 10)*, Washington, DC. USENIX Association.

Rocchetto, M. and Tippenhauer, N. O. (2016). CPDY: Extending the Dolev-Yao attacker with physical-layer interactions. In Ogata, K., Lawford, M., and Liu, S., editors, *Formal Methods and Software Engineering*, pages 175–192, Cham. Springer International Publishing.

Schaller, P., Schmidt, B., Basin, D., and Capkun, S. (2009). Modeling and verifying physical properties of security protocols for wireless networks. In *2009 22nd IEEE Computer Security Foundations Symposium*, pages 109–123.

Shen, W., Ning, P., He, X., and Dai, H. (2013). Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time. In *2013 IEEE Symposium on Security and Privacy*, pages 174–188.

Tippenhauer, N. O. and Čapkun, S. (2009). ID-based secure distance bounding and localization. In Backes, M. and Ning, P., editors, *Computer Security – ESORICS 2009: 14th European Symposium on Research in Computer Security, Saint-Malo, France, September 21-23, 2009. Proceedings*, pages 621–636. Springer Berlin Heidelberg, Berlin, Heidelberg.

Tippenhauer, N. O., Malisa, L., Ranganathan, A., and Capkun, S. (2013). On limitations of friendly jamming for confidentiality. In *2013 IEEE Symposium on Security and Privacy*, pages 160–173. IEEE Computer Society Press.

Xu, W., Trappe, W., Zhang, Y., and Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '05, pages 46–57. ACM, New York, NY, USA.

Zenger, C. T., Pietersz, M., and Paar, C. (2016). Preventing relay attacks and providing perfect forward secrecy using PHYSEC on 8-bit μC. In *2016 IEEE International Conference on Communications Workshops (ICC)*, pages 110–115.

ZigBee Alliance (2012). *ZigBee Light Link Standard Version 1.0 – Document 11-0037-10.*