Constructive and Destructive Aspects of Adaptive Wormholes for the 5G Tactile Internet

Christian T. Zenger[1,2], Jan Zimmer[2], Mario Pietersz[1,2],
Benedikt Driessen[1,2], and Christof Paar[2]
[1]PHYSEC GmbH, Universitätsstr. 150, 44801 Bochum, Germany
{christian.zenger, mario.pietersz, benedikt.driessen}@physec.de
[2]HGI, Ruhr-University Bochum, Germany
{jan.zimmer, christof.paar}@rub.de

ABSTRACT

In this work, we constructively combine *adaptive wormholes* with *channel-reciprocity based key establishment* (CRKE), which has been proposed as a lightweight security solution for IoT devices and might be even more important for the 5G Tactile Internet and its embedded low-end devices. We present a new secret key generation protocol where two parties compute shared cryptographic keys under narrow-band multi-path fading models over a delayed digital channel. The proposed approach furthermore enables distance-bounding the key establishment process via the coherence time dependencies of the wireless channel. Our scheme is thoroughly evaluated both theoretically and practically. For the latter, we used a testbed based on the IEEE 802.15.4 standard and performed extensive experiments in a real-world manufacturing environment. Additionally, we demonstrate adaptive wormhole attacks (AWOAs) and their consequences on several physical-layer security schemes. Furthermore, we proposed a countermeasure that minimizes the risk of AWOAs.

1. INTRODUCTION

We are in the midst of a collective movement towards the Internet of Things (IoT). Myriads of resource-constrained network nodes will communicate with each other, forming a wide spectrum of applications. A large number of IoT systems will be sensitive, e.g., automotive controllers, medical devices, SCADA systems, and many other cyber-physical systems. It is thus paramount that future IoT applications are equipped with security mechanisms.

A considerable portion of IoT devices can be characterized as resource-constrained platforms. Due to the fact that cheap platforms often do not provide true random number generators (TRNGs)—or efficient mechanisms for the statistical evaluation of randomness—and no secure storage for keys, security concepts based on pre-shared secrets or asymmetric cryptography do not fit very well. Furthermore, the calculation of discrete modular exponentiations or point multiplications on an elliptic curve is $\mathcal{O}(n^3)$ where n is the size of the desired key. Enabling dynamic encryption keys on low-end devices is, therefore, still one of the most difficult challenges.

Channel-reciprocity based key establishment (CRKE) is a practice-oriented secret-key agreement mechanism and part of the *physical layer security* (PHYSEC) family [9]. Recently, CRKE has been proposed as a potential lightweight solution for low-end IoT devices due to its linear complexity [38, 47, 49]. CRKE's low complexity results in low latency, which is one key-requirement for the Tactile Internet. Enabling the Tactile Internet is a main objective of the 5G Initiative [4]. The Tactile Internet is another paradigm shift lying ahead; it is motivated by the idea of controlling real and virtual objects in real-time via tactile feedback. A breakthrough is immanent once the latency of communication systems becomes low enough to enable round trip delays (from the input device through the network and back) of approximately 1 ms [13]. Areas in our life in which the Tactile Internet will have an important impact are health and care, education and sports, traffic, free-viewpoint video, smart grid, as well as robotics and manufacturing.

While promising in terms of latency, running CRKE over a purely digital channel (e.g., the Internet) was not possible so far. This changes when *adaptive wormhole attacks* (AWOA) are used in a constructive manner, as will be demonstrated later. Adaptive wormholes were introduced in theory as a potential attack against hidden wormhole detection mechanisms [23]. The attacker tricks the channel-based wormhole detection mechanism of two parties to believe they are communicating directly using the same physical channel. To do so, an adaptive wormhole works as a relay[1] that reactively adapts the transmission signal to manipulate channel estimations. Wormhole attacks are especially critical for distance-bounded applications (e.g., where a specified transmission range is used as a trust boundary), routing protocols of MANETs, and for CRKE as well. However, we identified adaptive wormholes as a security primitive which might have constructive applications, especially for IoT and low-latency technology such as 5G.

WiSec'16, July 18–20, 2016, Darmstadt, Germany.

DOI: http://dx.doi.org/2939918.2939923

[1]We note that relay attacks have been similarly applied in mobile ad-hoc networks (MANET), where they are known as wormhole attacks [17].

In this paper, we make the following contributions:

- We attacked two wormhole detection mechanisms and ten CRKE systems and present evaluation results.
- To the best of the author's knowledge, we present the first adaptive wormhole attack implementation.
- We present a new protocol that connects adaptive wormholes with CRKE. The wormhole is used to bridge digital channels for key establishment over the Internet and allows to achieve perfect forward secrecy based on a pre-distributed secret.

Prior work, as well as our prototypes are based on the popular IEEE 802.15.4 standard, frequently used in short-range industrial wireless sensor networks. We performed an extensive measurement campaign in a real-world industrial environment.

2. BACKGROUND

In this section, we characterize properties of a narrowband wireless channel and introduce constructions based on these.

2.1 Wireless Channel Primitives

The design of PHYSEC mechanisms, hidden wormhole attacks, as well as of wormholes detection mechanisms are based on features of the physical wireless channel. Therefore, we summarize three important properties of a radio channel, which can be assumed to be given in indoor environments.

2.1.1 Symmetry

The first key feature of a wireless channel is its symmetry, which can be exploited and utilized. Without taking noise, interference, and non-linear components into account, this symmetry relies on the principles of *antenna reciprocity* [33] and *channel reciprocity* [42]. In other words, the channel between A and B behaves similarly for transmissions from A to B and B to A. While antenna reciprocity is high and constant, a symmetric observation by A and B is only given if both channel measurements are done within a short period. This period is called *coherence time* and is highly dependent on the environment and movement within the transmission range. For most practical channels, these reciprocity properties hold and are easily observed [2].

2.1.2 Diversity

The second property of a radio channel is its spatial decorrelation or *channel diversity*: If uniformly distributed scatterers are given and channel variations occur, such as, due to moving scatterers, transmitters or receiver nodes, the spatial decorrelation is determined by a zero-order Bessel function. Here the first zero crossing of the correlation is given after approx. $\lambda/2$, where λ is the wavelength of the carrier signal [8]. Therefore, the correlation between a channel shared by A and B and a channel between A and C exhibits a distance-dependent behavior (cf. Fig. 1). However, an open research question is how the channel (de-)correlation behavior looks like if the requirements are not fully given (e.g., scatterers are not uniformly distributed). We do not tackle this question in this work, we rely on recent work showing that passive attacks are highly environment specific and only rarely successful [29, 20, 12, 47].

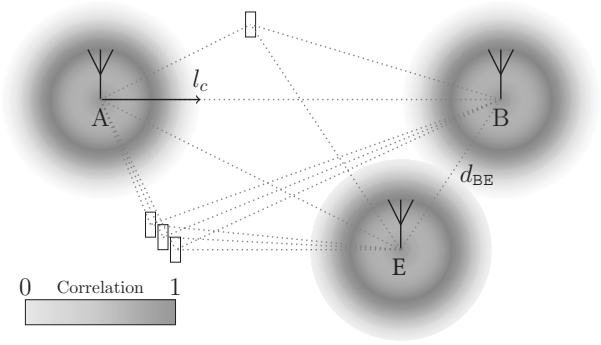


Figure 1: Simplified channel model: The spatial channel (de-)correlation versus distance is illustrated for each node. Further, because of the complex, time-varying environment, all channels are independent.

2.1.3 Randomness

The third key feature is the randomness of a radio channel. A complex and dynamic environment leads to unpredictable wave propagation effects, such as diffraction, scattering, and reflection. As a result, channel measurements between two parties A and B are location-specific, reciprocal, and time-varying. A wireless channel can thus serve as entropy source for cryptographic solutions. However, this requires a secure modus operandi in the case of entropy loss as well as a thorough evaluation of the physical source of randomness. Depending on the application, on-line statistical testing is an essential ingredient in order to detect statistical defects during runtime [48].

2.2 Channel-Reciprocity Based Key Extraction

As mentioned above, an alternative approach to key agreement is based on PHYSEC, which exploits physical features of wireless communication. In particular, the inherent randomness of the wireless medium can be utilized to establish a shared secret. This approach is referred to as CRKE and is characterized by three parties A, B, and E which observe a *discrete memoryless source* (DMS). The observations of A and B are assumed to contain mutual information, which is not or only partly shared with E. Entropy not shared with E is called the secret-key capacity of the DMS. Furthermore, it is assumed that the DMS is not predictable or malleable in a way that E can guess $A's$ and $B's$ observations. See Figure 1 for the general model.

The approach is based on the quasi-simultaneous measurement of the wireless channel by A and B. Afterwards, measurements are post-processed, quantized, and error corrected in order to remove noise and interferences. The resulting entropy is collected and utilized as a shared symmetric key. Besides providing shared randomness, the scheme is also inherently secure to attacks. If E's distance to both legitimate nodes is large enough, her observation of the channel is uncorrelated with the observations of A and B and thus an attack is not possible.

The general feasibility of the approach has been reported by extensive prior work [37, 26, 44, 32, 5, 6, 29, 20, 31, 27, 3, 46, 14, 29, 45, 50, 41, 43]. The first practice-oriented protocol for the unconditionally secure extraction of a symmetric key over public wireless fading channels was introduced by

Tope et al. [37] in 2001. Based on his approach, many protocols for key extraction have been proposed. One CRKE family is based on received signal strength indicators (RSSIs) [5, 6, 29, 20, 31, 27, 3, 46]. RSSI-based systems are very attractive because virtually every wireless communication interface provides RSSI values on a per packet basis. Another family exploits the channel impulse response (CIR) as a more general estimate [14, 29, 45, 50]. Other variants are based on channel phase randomness [41] or frequency hopping [43]. Mathur et al. [29] and Jana et al. [20] included brief thoughts on potential attacks in their proposals. Simple countermeasures against spoofing attacks by active adversaries were introduced by Mathur et al. [29] and Ye et al. [45]. There has also been some work that deals with temporal correlation of samples, such as principal component analysis [10], beamforming [28] or linear prediction [30].

2.3 (Adaptive) Wormhole Attacks

In many use cases (e.g., remote keyless entry systems, MANET routing protocols, or future Tactile Internet applications) correctly estimating the distance of two communication parties is crucial. In the absence of such possibilities, a wormhole attacker can trick two communication parties into believing they are close, when in fact they are not. These attacks exploit the flawed assumption that the ability to wirelessly communicate with a party guarantees its proximity.

Jain et al. [19] proposed a technique which exploits the reciprocity of RSSIs in order to detect wormhole attacks. Specifically, the property being leveraged is that, when two nodes communicate through a wormhole, their channel measurements will be uncorrelated with high probability. The approach is based on key extraction schemes with relaxed requirements (because no cryptographic key needs to be established). Krentz et al. build upon this with their own variant for 6LoWPAN, which uses channel hopping and randomized transmission powers [23]. They furthermore describe an AWOA that aims to be undetectable by past detection algorithms including Krentz et al.'s scheme itself.

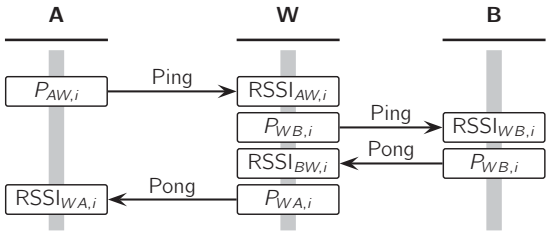


Figure 2: The adaptive wormhole attack, which was introduced by Krentz et al. [23].

The basic scenario is shown in Figure 2. The goal for an attacker is to recreate equal (or highly correlated) RSSI measurements for A and B so that a wormhole attack cannot be detected. Equal transmission power $P_{AB,i} = P_{BA,i}$ is assumed here. There is a relationship $RSSI = P - L$, with P being transmission power and L path loss. Path loss is the reduction in power density of an electromagnetic wave as it propagates through space. This is a function of the travel distance of the wave as well as of fluctuations due to large-scale and small-scale fading. We define that $L_{1,i}$ and $L'_{1,i}$ is the path loss from A to W, and vice versa. Further, we define that $L_{2,i}$ and $L'_{2,i}$ is the path loss from B to W, and vice versa. This leads to the following equations:

$$RSSI_{WA,i} - RSSI_{WB,i} = P_{WA,i} - P_{WB,i} - L'_{1,i} + L_{2,i}$$
$$RSSI_{AW,i} - RSSI_{BW,i} = P_{AW,i} - P_{BW,i} - L_{1,i} + L'_{2,i}$$

Due to channel reciprocity we can assume that $L_{1,i} \approx L'_{1,i}$ and $L_{2,i} \approx L'_{2,i}$, thus:

$$RSSI_{WA,i} - RSSI_{WB,i} \approx RSSI_{AW,i} + P_{WA,i} - P_{AB,i} - RSSI_{BW,i} - P_{WB,i} + P_{BA,i} \quad (1)$$

Now the i'th PONG is forwarded by W with the transmission power $P_{WA,i}$ chosen as:

$$P_{WA,i} = P_{WB,i} + RSSI_{BW,i} - RSSI_{AW,i}. \quad (2)$$

Combining Equation 1 and 2 we get the results $RSSI_{WA,i} \approx RSSI_{WB,i}$, which leads to the wormhole being undetected (Jain et al.'s channel reciprocity metrics show high values, which results in false negatives). The attack was designed to attack routing protocols of IPv6-based WSNs. However, it can also be used to attack future latency (or hop count) critical network, novel remote keyless entry systems as well as CRKE schemes.

2.4 Evaluation Metrics

Throughout this paper, we use the Pearson correlation, mutual information and the secret-key rate as evaluation metrics for achievable security levels.

2.4.1 Pearson correlation

The Pearson correlation provides a measure of linear dependency between two data series. For PHYSEC, it was introduced for the analysis of coherence time behavior as well as for analyses of the performance of quantization schemes. Correlation values are between -1 and 1, where 1 refers to absolute correlation, 0 to no correlation, and -1 to perfect inverse correlation. Given a finite collection of N pairs (x_i, y_i) we use the following estimator:

$$\rho_{xy} = \frac{\sum_{i=0}^{N-1} (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=0}^{N-1} (x_i - \bar{x})^2} \sqrt{\sum_{i=0}^{N-1} (y_i - \bar{y})^2}}, \quad (3)$$

where $\bar{x} = \frac{1}{N} \sum_{j=0}^{N-1} x_j$ and $\bar{y} = \frac{1}{N} \sum_{j=0}^{N-1} y_j$ are the sample means of x_i and y_i, respectively.

2.4.2 Mutual Information

Mutual information is a general metric for the dependency between two random variables. It is a function of joint and marginal probability densities. We utilize a k-nearest neighbor estimator (kNNE) to estimate the mutual information, which is based on the idea and implementation of Kraskov et al. [22]. For a measure of the joint density, the estimator computes the distance between a tuple of samples and its kth-nearest neighbors. A similar approach is provided for the marginal densities. We use the mutual information estimator also to estimate the entropy $H(X) = I(X; X)$.

2.4.3 Secret-Key Rate

Based on the mutual information metric, a lower bound on the secret-key capacity of a channel in the source-model can be applied under the following conditions:

1. The joint probability density function is known a priori at all channel end-points.
2. Alice and Bob exchange messages over an authenticated, public channel with unlimited communication capacity, e.g., over the Internet.
3. Eve remains passive at all times.

Subsequently, the asymptotic bound is given by

$$C_{sk}(X;Y;Z) \geq I(X;Y) - \min\left[I(Y;Z), I(X;Z)\right],$$

since the process is stationary [1].

The lower bound $R_{sk}(X;Y;Z)$ is evaluated by estimations based on a finite number of measured samples and gives the secret-key capacity of a channel.

3. AWOUR - ADAPTIVE WORMHOLE BASED UNTRUSTED RELAY

In this section, we introduce the *Adaptive WOrmhole based Unstrusted Relay* (AWOUR) protocol for secret-key establishment. With this novel protocol, fresh key material (or joint entropy not shared with others) can be established between two authenticated devices over two-way, untrusted relayed, and delayed channels (TW-UR-DC). To do so, the mechanism utilizes CRKE and adaptive wormholes. Additionally, the scheme enforces a maximum delay which makes it interesting for distance bounding applications. The approach is particulary suitable for embedded devices without a secure clock or applications where the physical distance between both parties is important.

AWOUR is based on the time dependent amount of reciprocity between bidirectional measurements. The reciprocity can be estimated using the Pearson correlation. Furthermore, the minimum correlation required to perform CRKE can be determined [48]. In this context, the duration between channel measurements by the two communication partners is defined as the coherence time. As we show later in this section, the channel can be interpreted as a stationary random process with *adjustable coherence times*.

3.1 Protocol

The goal of the protocol is to continuously generate fresh secret keys, known only to A and B, in order to achieve *perfect forward secrecy* (PFS). However, A and B do not share the same physical channel. Instead, A communicates with W_1 and W_2 with B via a reciprocal channel. W_1 and W_2 are the two end-points of a wormhole, connected with each other over a delayed digital channel, see Figure 3. The protocol requires a previously distributed symmetric key k_0, known to only A and B. This key is assumed to be established during an earlier phase, e.g., when both devices were in proximity and executed a PHYSEC-based pairing protocol.

The general protocol works like this: Initially, A and B use k_0 and a public constant c_0 to generate a sequence of random power levels:

$$\begin{aligned} f_1(k_0, 0) &= \{P_{A,0}, P_{A,1}, ...\} \quad \text{and} \\ f_1(k_0, c_0) &= \{P_{B,0}, P_{B,1}, ...\} \quad \text{with} \quad c_0 \neq 0. \end{aligned}$$

Care needs to be taken that these values are in the set $\mathbb{P} \subset Z$ of power levels supported by the participating devices, i.e., $P_{AW_1,i}, P_{BW_2,i} \in_R \mathbb{P}$.

For each pair $(P_{AW_1,i}, P_{BW_2,i})$ and $0 \leq i < N$ the parties A and B can execute a PING-PONG protocol to extract shared entropy from the local channels between A and W_1 and W_2 and B. For this, A uses power level $P_{AW_1,i}$ and sends a PING to W_1 over the reciprocal channel. W_1 measures $RSSI_{AW_1,i}$ and relays it (together with the message) to W_2 over the digital channel. W_2 uses power level $P_{W_2B,i} = f_2(RSSI_{AW_1,i})$ and sends the PING to B where $RSSI_{W_2B,i}$ is measured. On the way back, B sends PONG to W_2 using $P_{BW_2,i}$. W_2 measures $RSSI_{BW_2,i}$ and relays it to W_1 with $P_{W_1A,i} = f_2(RSSI_{BW_2,i})$. Finally, the PONG reaches A, where $RSSI_{W_1A,i}$ is measured.

The previously introduced relationship $RSSI = P - L$ leads to the following equations:

$$RSSI_{AW_1,i} = P_{AW_1,i} - L_{1,i} \tag{4}$$
$$RSSI_{BW_2,i} = P_{BW_2,i} - L_{2,i} \tag{5}$$

We also have the following:

$$\begin{aligned} RSSI_{W_1A,i} &= P_{W_1A,i} - L'_{1,i} \\ &= f_2(RSSI_{BW_2,i}) - L'_{1,i} \\ RSSI_{W_2B,i} &= P_{W_2B,i} - L'_{2,i} \\ &= f_2(RSSI_{AW_1,i}) - L'_{2,i} \end{aligned}$$

If we define $\mathbb{R} \subset \mathbb{Z}$ as the range of RSSI values measurable by the participating devices, then we have

$$f_2 : \mathbb{R} \to \mathbb{P},$$

i.e., a mapping from RSSIs to power levels. We define $RSSI_{W_1,max}, RSSI_{W_2,max}$ as the maxima of the actually occuring RSSIs for W_1 and W_2 and $RSSI_{W_1,min}, RSSI_{W_2,min}$ as the respective minima, i.e.,

$$\begin{aligned} RSSI_{W_1,min} \leq RSSI_{AW_1,i} \leq RSSI_{W_1,max}, \\ RSSI_{W_2,min} \leq RSSI_{BW_2,i} \leq RSSI_{W_2,max}, \end{aligned}$$

for all $0 \leq i < N$. Assuming that

$$\begin{aligned} |RSSI_{W_1,max} - RSSI_{W_1,min}| + 1 \leq |\mathbb{P}| \quad \text{and} \\ |RSSI_{W_2,max} - RSSI_{W_2,min}| + 1 \leq |\mathbb{P}| \end{aligned}$$

holds (and $\mathbb{P}$ and $\mathbb{R}$ are consecutive), we can say that

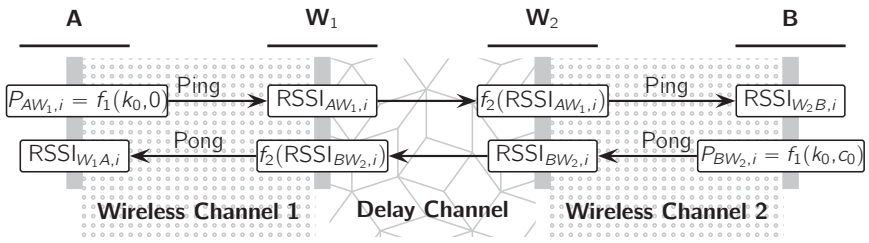
$$\begin{aligned} P_{W_2,i} = f_2(RSSI_{AW_1,i}) \approx RSSI_{AW_1,i} + c_1 \quad \text{and} \\ P_{W_1,i} = f_2(RSSI_{BW_2,i}) \approx RSSI_{BW_2,i} + c_2 \end{aligned}$$

holds as well, where c_1 and c_2 are public constants. If A or B may move the constants may change over time.

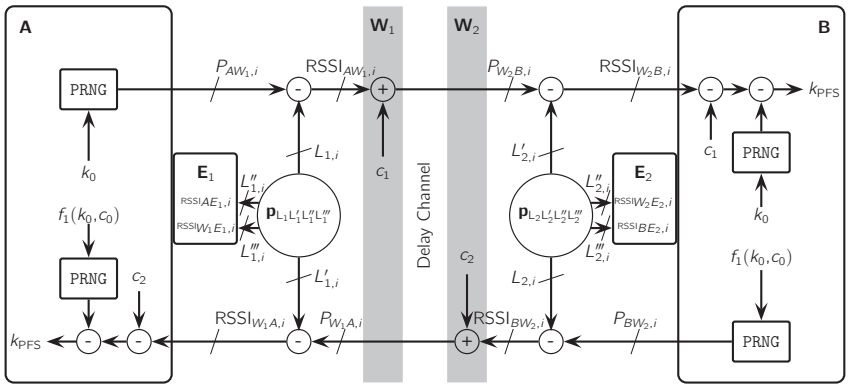
Combining all this—and given that A knows $P_{BW_2,i}$ and B knows $P_{AW_1,i}$ due to shared knowledge of k_0—we find that due to

$$RSSI_{W_1A,i} - P_{BW_2,i} - c_2 = -L_{2,i} - L'_{1,i} \quad \text{and} \tag{6}$$
$$RSSI_{W_1B,i} - P_{AW_1,i} - c_1 = -L_{1,i} - L'_{2,i} \tag{7}$$

both have access to a common entropy source not shared with others. A and B can then use this entropy source to establish keys with well-known CRKE protocols. We discuss the results of 10 different approaches from the literature in Section 4.5. To hold the pre-shared authenticity, the key k_0 could be used in the derivation of the final session key.



(a) Protocol view.



(b) Model view.

Figure 3: AWOUR protocol for secret key generation over a digital channel.

3.2 Security Analysis

The goal of an adversary Oskar O is to obtain either the key k_{PFS} directly or information about the path losses $L_{1,i} \approx L'_{1,i}$ and $L_{2,i} \approx L'_{2,i}$ such that he can reconstruct the key.

Denial of service attacks are not considered.

3.2.1 Untrusted Wormhole (UW)

The untrusted wormhole (UW) attacker O_{UW} has full access to $RSSI_{AW_1,i}$ (Eq. 4) and $RSSI_{BW_2,i}$ (Eq. 5). However, $P_{A,i}$ and $P_{B,i}$ are independent and unknown to O_{UW}, furthermore $L_{1,i}$ and $L_{2,i}$ are uncorrelated and unpredictable as well. Therefore, the attacker cannot extract the secret channel parameters $L_{1,i}$ and $L_{2,i}$ out of the measured values.

3.2.2 Passive Eavesdropper (PE)

Both bidirectionally communicating devices (here A and W_1 as well as W_2 and B) are using the channel-reciprocity to access the common entropy ($L_{1,i}$ and $L_{2,i}$). The attackers O_{PE_1} and O_{PE_2} are able to measure these values:

$$\begin{aligned} RSSI_{AE_1,i} &= P_{AW_1,i} - L''_{1,i}, \\ RSSI_{W_1E_1,i} &= P_{W_1A,i} - L'''_{1,i}, \\ RSSI_{BE_2,i} &= P_{BW_2,i} - L''_{1,i}, \\ RSSI_{W_2E_2,i} &= P_{W_2B,i} - L'''_{1,i}. \end{aligned} \tag{8}$$

where L'' and L''' are their observations (cf. Fig. 3). Because $L_{1,i}$ and $L_{2,i}$ are independent, their secret-key capacity can be estimated separately. Due to spatial diversity, complex environments, and random physical processes within the transmission ranges, we assume that the secret-key rate is larger than zero. Therefore, secret-key extraction is assumed to be possible. Furthermore, the attackers need to perform the eavesdropping attack simultaneously at both locations.

Existing literature provides different analyses with varying results for passively eavesdropping on CRKE [32, 5, 6, 29, 20, 31, 46, 14, 29, 43]. Successful attacks—attacks with low secret-key rate due to observation—have in common that special-cases need to be created and a *sweet spot* position for attacker's antenna need to be found.

3.2.3 Known Key$_0$ (KK_0) Attacker

For the O_{KK_0} attacker we assume a rather strong attacker, who can extract the pre-shared secret k_0 before the re-keying/entropy collection protocol starts. Key extraction per se is a realistic attack because it is easy to dump the memory of low-end devices without secure storage. The attacker's goal is still to obtain the new secret key, instead of performing an impersonating attack. O_{KK_0} is of course able to reproduce the pseudo random variables $P_{AW_1,i}$ and $P_{BW_2,i}$. However, without further knowledge (e.g., $RSSI = P - L$) he is not able to guess either the key k_{PFS} or path losses, e.g., L_1 and L_2, because P and L are independent. Since the pre-shared trusted relationship between the nodes is broken at this point, attacks on the authenticity can be carried out by a MitM attack. However, the attack is different to the previous discussed, since the MitM exchanges different keys with each party and only relays information as required.

3.2.4 UW-KK_0 Attacker

Next we consider the attacker O_{UW-KK_0}, combining the capabilities of O_{KK_0} and O_{UW}. This is a rather strong attacker because he has to extract k_0 directly after its establishment and simultaneously gets access to a wormhole gateway before sufficient entropy was collected. Zenger et al. [48]

have shown that 128 bit keys, which are verified by a NIST on-line entropy estimation suite [7], can be established within 58 s, therefore this time window is very narrow.

With knowledge of k_0 the attacker can reproduce $P_{AW_1,i}$ and $P_{BW_2,i}$, then he measures $RSSI_{AW_1,i}, RSSI_{BW_2,i}$ and can thus extract $L_{1,i}$ and $L_{2,i}$ (see Eq. 4 and Eq. 5). Because the mutual information $I(L_1, L_1')$ and $I(L_2, L_2')$ is high per definition, the attacker can thus obtain the key k_{PFS} (see Eq. 6 and Eq. 7).

4. IMPLEMENTATION AND EVALUATION

In this section, we describe a use cases driven evaluation of adaptive wormholes. In Section 4.1, we present a test environment that corresponds to a real-world environment as much as possible in order to minimize the risk of environment-specific failures not being found during testing. Our contribution is really the prototyping of the adaptive wormhole system for the random source of interest (wireless channels), the evaluation of the random process involved, and the presentation of results for several CRKE-quantization schemes. Our prototype testbed is presented in Section 4.2. In Section 4.3 and Section 4.4, we describe properties of the random sources, and real-world restrictions of the testbed. In Section 4.5, we provide results of the AWOA as well as results and discussion for our proposed secret key generation system.

4.1 Use Case and Environment

We address an example application which requires PFS: sensor readings for industrial automation. Confidentiality of sensor readings is important because they contain information about the intellectual property of its operators. Furthermore, integrity of sensor data needs to be protected against manipulation by saboteurs.

We executed our experiments in a 400 qm production hall equipped with housing manufacturing tools and robots for metal processing. Three kinds of industrial sensors are already in use: electrical energy measuring sensors, air pressure sensors, and cooling lubricant consumption sensors. Sensor readings are currently transported via cable and used to control and improve manufacturing processes.

For several reasons, future sensors will provide their readings wirelessly. For example, wireless sensors have a unique advantage over traditional sensors. They enable the mounting at almost any position and drastically simplify installation. Upgrading existing manufacturing facilities with wired sensors is a hassle today: the installation requires drilling new holes and running wires across the facility, which is typically avoided at all costs. Furthermore, cable ducts require advanced fire protection and further qualifications, which, again, is expensive and takes time.

In the facility at hand, wireless communication systems are used for the communication between Programmable Logic Controllers (PLCs) of different machines and a PCL head control. Our testbed systems as well as the PLC communication system use the 2.4 GHz ISM band, however, the channels are not overlapping. Our testbed gateway A is positioned next to the head control gateway (cf. Figure 9 (g)). The head control gateway forwards sensor reading via wire to the head control. Six testbed nodes B_k are located at across the facility, close to actual sensors.

4.2 Testbed to measure Joint Stationarity

We perform bidirectional, narrow-band short-range channel measurements on 2.4 GHz (wavelength 12.5 cm) based on the IEEE 802.15.4 standard. We use Texas Intruments CC2530 modules to access the physical layer and combine them with Raspberry PI 2 devices, where the higher-levels of our measurement logic are implemented. The IEEE 802.15.4 standard is suited for energy-constrained device, such as mobile sensors and electronic keys. The CC2530 is a SoC designed for 20-years battery life and compatibility to network layer standards for resource-constrained devices: ZigBee, WirelessHART, and 6LoWPAN. WirelessHART, and 6LoWPAN are network standards which were introduced for industrial applications. The CC2530 is built around the 8051 processor with 8-bit data paths. Furthermore, it is equipped with a proprietary 5 mm × 12 mm *Meandered Inverted-F antenna* (MIFA) which provides good performance with a small form factor. The platform and antenna design is widely used in commercial products and suited for systems where ultra-low power consumption is required.

In order to establish common channel probing, the gateway W periodically sends data frames to receivers B_k and waits for acknowledgments. When receiving a probe, all devices extract RSSI values and, thus, can measure a channel-dependent sequence over time. We perform N reciprocal measurements v_i between W and nodes $B_0, B_1, ..B_5$, each of these producing a set of six tuples

$$v_i = \{ \; (RSSI_{WB_0,i}, RSSI_{B_0W,i}), \; (RSSI_{WB_1,i}, RSSI_{B_1W,i}), ...\}$$

where $RSSI_{WB_0,i}$ denotes value for the channel between W and B_0 on B_0's side, whereas $RSSI_{B_0W,i}$ denotes the result of the quasi-simultaneous measurement at W's end.

The CC2530 provides 7-bit RSSI values within the range of −100 dBm to 20 dBm and, further, transmission power levels between −25 dBm and 3 dBm, both with 1 dBm resolution. Note than only 16 different power levels are documented[2], however, we figured out that more transmission power levels are configurable by using intermediate values of the official transmission power register settings. IEEE 802.15.4 transceivers provide software and hardware acknowledgments, which are used in our setup for the PONGS. The round trip time (RTT) of the PING-PONGS is ≈3.5 ms using software and ≈1 ms for hardware acknowledgments. As we will see later, the RTT is crucial for achieving highly correlated measurements. However, through the use of software acknowledgment frames a reactive transmission power adoption is possible.

We obtain a complete set $\mathbf{v_i}$ for every sampling interval. The setup is able to adapt the interval between two PING-PONGS down to $T_s = 6.25ms$. However, we use a sampling interval of $T_s = 50ms$, if it is not otherwise specified. Further, the protocol ensures that gateway and end-device can probe the channel within a probing duration $T_p \approx$ 1 msec using hardware acknowledgments. The gateway and all six nodes extract the common randomness $RSSI_{WB_k,i}$ and $RSSI_{B_kW,i}$ from a time-varying channel. Since we aim for meaningful and reproducible results, we have to create an environment which provides joint stationarity to the random process. Therefore, with a distance of 10 cm to gateway's antenna, we deploy a curtain of 30 × 30 cm aluminum strips

[2]http://www.ti.com/tool/cc2531emk

that continuously rotates at ≈ 0.1 rotations per second, cf. Figure 9 (h).

However, continuous rotation itself inserts a deterministic component into the channel which is illustrated in Figure 4. It shows that the mutual information decays rapidly and vanishes after four samples, corresponding to approximately 400 ms. However, due to the continuously rotating curtain of aluminum strips, we discover strong stochastic dependencies after 96 samples, corresponding to approximately 9.6 seconds. To solve this problem, we randomize the direction and angle intervals of the rotating curtain. We applied five different speed levels as summarized in Table 2. Figure 4 shows that no strong stochastic dependencies are given anymore for random rotation.

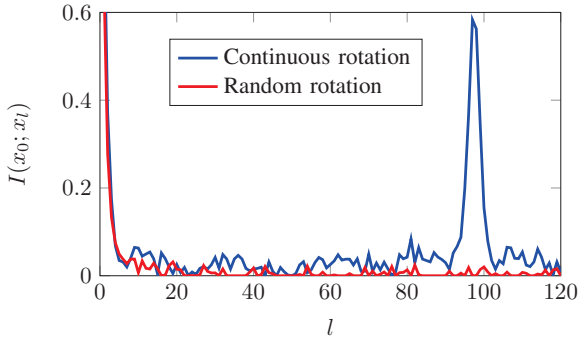


Figure 4: Self-dependence of RSSI values with respect to time delay. Setup is equipped with curtain of aluminum strips, rotating either continuously or randomly.

Next we analyzed six simultaneous measurements using different sensor positions. The results we present are representative for the different speed levels of the randomized curtain as well as for different transmission power levels. For the latter, the average receiving power of course changes. The probability density function of the received RSSI values are Rayleigh distributed. The mean value of the measurements differs due to the sensor testbed's positions. For this experiment, the randomized curtain runs at a mean angular-speed of 1.047 rad/s. We use transmission power levels of 3 dBm for the best case and -25 dBm for the worst case. The mutual information as well as the Pearson correlation ρ between channel measurements $RSSI_{WB_k,i}$ and $RSSI_{WB_l,i}$, with $k, l \in \{0, 1, ..5\}$ and $k \neq l$, of different sensor nodes are always low ($\rho_{max} = 0.17$), which demonstrates the channel's spatial diversity with almost independent measurement results. The mutual information and Pearson correlation between Ping-Pongs ($RSSI_{WB_k,i}$ and $RSSI_{B_kW,i}$) is high due to channel reciprocity ($\rho_{max} = 0.94$). The secret-key rate is positive for both transmission power levels. While for the best case more than 3 Bit can be extracted securely, for the worst case it is only 0.8 Bit. Detailed results are summarized in Table 1.

4.3 Coherence Time of the Channel

To estimate the channel reciprocity behavior over time, we sampled the channel with the highest possible rate of our testbed, which is $r_s = T_s^{-1} = 160$ bidirectional packets per second. Then we calculated the Pearson correlation between the original and the delayed samples. We repeated the experiment for different speeds (on average) levels of the aluminum strips based random process generator. The correlation versus sampling delays is illustrated in Figure 5. It shows that the reciprocity steadily decreases as probing delays increase. The (de-)correlation courses (slope of the curves) clearly demonstrate the relationship between the coherence time and the chosen speed level. For example, we identified the two coherence times $t_{c,\rho=0.9}$ and $t_{c,\rho=0.8}$ for cross-correlations of $\rho(X, X_{delayed}) = 0.9$ and $\rho(X, X_{delayed}) = 0.8$, respectively. In Table 2, we summarize the coherence time results for all five speed levels. For $t_{c,\rho=0.8}$, the results show that a 62 ms probing delay in the 1.047 rad/s speed level is equivalent to a 142 ms probing delay in the 0.572 rad/s speed setup, as well as equivalent to a 397 ms probing delay in the 0.241 rad/s speed setup. Therefore, results confirm the intuition that the speed levels of the randomized generator influence coherence times of the resulting measurements.

Table 1: Worst case results of measurements using constant transmission power.

	$TX = 3$ dBm	$TX = -25$ dBm
$H(X) = H(RSSI_{WB_k})$	4.4096 bit	1.9844 bit
$H(Y) = H(RSSI_{B_kW})$	4.3943 bit	2.1897 bit
$H(Z) = H(RSSI_{WE})$	3.7004 bit	2.3337 bit
$I(X;Y)$	3.2876 bit	0.8543 bit
$I(X;Z)$	0.1169 bit	0.0397 bit
$I(Y;Z)$	0.1201 bit	0.0474 bit
$R_{sk}(X,Y,Z)$	3.1707 bit	0.8146 bit

Table 2: Coherence time results.

Speed levels [rad/s]	$t_{c,\rho=0.9}$ [ms]	$t_{c,\rho=0.8}$ [ms]
$v_0 = 1.047$	21	62
$v_1 = 0.572$	42	142
$v_2 = 0.393$	61	156
$v_3 = 0.298$	142	294
$v_4 = 0.241$	177	397

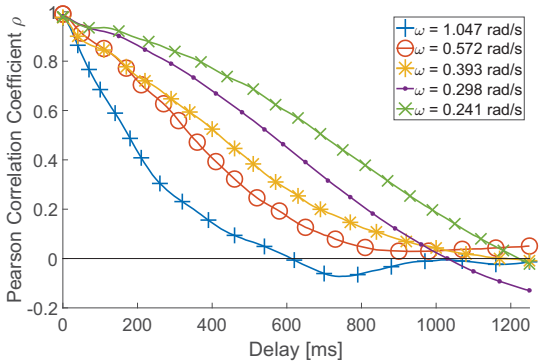


Figure 5: Correlation ρ versus sampling delay.

4.4 Adaptive Wormholes

Next, we analyze the performance of the AWOA in the testbed environment, where small-scale and large-scale fad-

ing effects as well as noise and interference occur. We performed different experiments to create and analyze adaptive wormholes across six sensor testbeds. Unfortunately, we were not able to sufficiently reduce the process time duration of the communication stacks between the first wormhole transceiver and the second one to make the system real-time capable. However, we describe a method how adaptive wormholes can still be evaluated for such applications.

For the performance analyses of the AWOUR protocol, we simulated the real-time adaptivity of the wormhole between both wormhole ends. The CC2530 testbeds provide 29 different power levels: $\{-25, ..., 3\}$ dBm. We generated six independent sensor-gateway series $\mathbf{v}_k^{TX_{S_k},TX_{G_k}}$ applying all possible 29×29 transmission power combinations, with $k \in \{0, 1, ...5\}$. The results allow us to include potential non-linear effects of both channels, of the transmission unit, and of the receiver unit, into the evaluation. The transmission power of G_k is TX_{G_k} and for S_k it is TX_{S_k}. Therefore, the received RSSI values of the receiving party are based on the transmission power level of the transmitting party: $\mathbf{v}_k^{TX_{G_k},TX_{S_k}} := \left(RSSI_{G_kS_k}^{TX_{G_k}}, RSSI_{S_kG_k}^{TX_{S_k}}\right)^T$. One sensor-gateway realization series can be represented by the matrix

$$\mathbf{v}_k^{TX_{G_k},TX_{S_k}} = \begin{bmatrix} \mathbf{v}_k^{-25,-25} & \mathbf{v}_k^{-25,-24} & \dots & \mathbf{v}_k^{-25,3} \\ \mathbf{v}_k^{-24,-25} & \ddots & & \mathbf{v}_k^{-24,3} \\ \vdots & & & \vdots \\ \mathbf{v}_k^{3,-25} & \mathbf{v}_k^{3,-24} & \dots & \mathbf{v}_k^{3,3} \end{bmatrix}.$$

For statistical reasons, each measurement representation contains $2 \cdot 100\,000$ RSSI values and, therefore, each series contains 135.2 million RSSI values. We used combinations of these individual sensor-gateway channels in the testbed to simulate the PING-PONG protocols between A and W_1 and W_2 and B.

Next, we want to address the physical limitations of our testbed. Because the actual transmission power range is limited to 29 distinct levels, the result of Equation 2 needs to be within this range to perform optimally. However, this is not always given. For example, in the case of creating a wormhole between two devices the average transmission power would be:

$$\begin{aligned} P_{WA,i} &= P_{WB,i} + RSSI_{WB,i} - RSSI_{WA,i} \\ &= 0\,\text{dBm} - 45\,\text{dBm} - (-90\,\text{dBm}) \\ &= 45\,\text{dBm}. \end{aligned}$$

Unfortunately, this power level cannot be reached with our low-cost testbed, even though this is not a principal problem in itself (it can be done with special hardware).

The worst case scenario is given if one party would be very close to the wormhole, e.g., $RSSI_{WB,i} = 0\,\text{dBm}$, and the other far away, e.g., $RSSI_{WA,i} = -90\,\text{dBm}$. Now the required transmission power is $P_{WA,i} = -90\,\text{dBm}$, which is, again, out of the possible range for our testbed. For such scenarios the adaptive wormhole attacker or the AWOUR wormhole needs to be within a comfort distance. In Figure 6 such a comfort zone is shown. With regard to the IEEE 802.15.4 standard we estimate the link budget for receiver power (and the corresponding distances) for optimal wormhole performance. To do so, we fix the sum of transmitter output power, transmitter and receiver antenna gain, as well as transmitter and receiver losses (mismatching etc.) to an on average value of $-20\,\text{dBm}$. Then Friis equation for path loss is applied $L_{FS} = 20\log(\frac{4\pi d}{\lambda})$, where L_{LS} is the free space path loss, λ is the wavelength of the carrier, and d is the distance between transmitter (victim) and receiver (attacker).

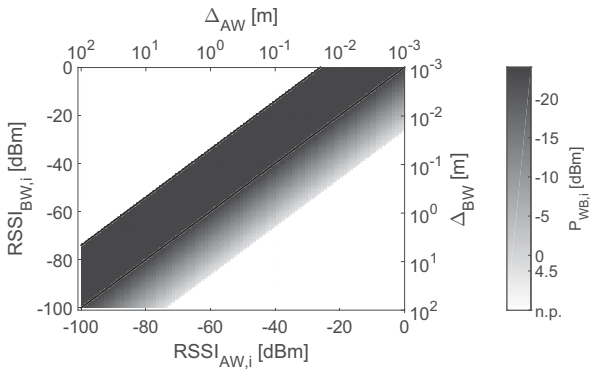


Figure 6: RSSI ranges of $RSSI_{BW,i}$ and $RSSI_{AW,i}$ to perform the AWOA optimally.

The linear relationship between transmission power and the corresponding RSSI value is of importance for the quality of the adaptive wormhole attacker and the AWOUR wormhole, as well. Figure 7 illustrates four different joint distributions of RSSI values of a $\mathbf{v}_{WB,i}$ measurement. The differences between the measurement sets are the transmission power levels we have used. The chosen power values are $\{-25, -12, -5, 3\}$ dBm. The resulting mean RSSI values are $\{-83, -73, -66, -56\}$ dBm. The variance of the error distribution over all measurements is 2.35. The figure also shows that the correlation is high, which is clearly visible by observing how little the results are spread out vertically within one set of measurements for a fixed power level.

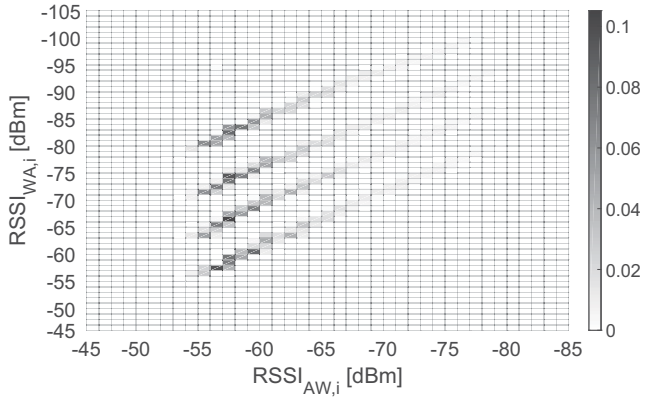


Figure 7: Joint distribution of $RSSI_{WA,i}$ and $RSSI_{AW,i}$ for four different reactively adopted transmission power levels of $P_{WA,i}$.

Next, we analyze the performance of recovering the channel profiles using single-side random transmission power. Therefore, we estimate the mutual information $I(X;Y)$ between $X = RSSI_{W_1A}^{TX=const.}$ and $Y = RSSI_{AW_1}^{TX=random} - P_{W_1A}^{random}$. The average $I(X;Y)$ for randomly chosen trans-

mission power levels is 2.5906. Compared to the best for a constant power level we lose ≈ 0.7 bit of mutual information; and win ≈ 1.7 bit compared to the worst case results. To analyze the capabilities of an attacker to separate the components, e.g.,$P_{AW_1,i}$ and $L''_{1,i}$ of the $Z = RSSI^{TX=random}_{E,i}$ he received, we estimate the mutual information $I(X;Z)$ and $I(Y;Z)$ as well as the secret-key rate $R_{sk}(X;Y;Z)$. With $I(X;Z) = 0.1983$ bit and $I(Y;Z) = 0.9544$ bit the secret-key rate is 2.3923 bit.

Finally, we analyzed the performance of the AWOA. Compared to our previous analyses the second channel L_2 added an additional error due to non-perfect reciprocity. The results show that the correlation $\rho(RSSI_{W_1A,i}, RSSI_{W_2B,i})$ (using the wormhole) is 0.91 and, therefore, only slightly lower than the correlation of $\rho(RSSI_{W_2B,i}, RSSI_{BW_2,i})$ (using the reciprocal channel measurements by direct link), which is 0.94. The mutual information between A and B is 1.8678 bit. Compared to the results of measurements using single-side, random transmission power reduces the mutual information by 0.7228 bit. Assuming a passive eavesdropper trying to attack the key generated using the adaptive wormhole, the scheme achieves a secret-key rate of R_{sk} of 1.3452 bit. This is 1.0471 bit less than using single-side random transmission powers.

For the performance evaluation of the AWOUR protocol we use two independent measurement series of $\mathbf{v}^{TX1,TX2}_{G_k,S_k,i}$ for wireless communication channels. The Pearson correlation between $RSSI^{TX=adap.}_{W_1A,i}$ and $RSSI^{TX=adap.}_{W_2B,i}$ is 0.8. The average entropy is $H(RSSI^{TX=adap.}_{W_1A}) = 4$. The mutual information of the shared key material is $I(-L_1-L'_2; -L'_1-L_2) = 1.015$. By introducing a passive eavesdropper into one of both channel, we achieve a secret-key rate of $R_{sk} = 0.4894$. The results show that the AWOUR protocol is capable to perform secret-key establishment using narrowband multipath fading channel.

Figure 8 shows exemplary the *probability density function* (PDF) of the overall measured RSSI values (dotted line). This PDF is composed out of several PDFs. These PDFs correspond to six different transmission power levels, which is only an exemplary subset. With this information the corresponding entropy (or uncertainty of an O_{UW} attacker) can be calculated. Determining the amount of entropy and the corresponding secrecy rate is left for future work.

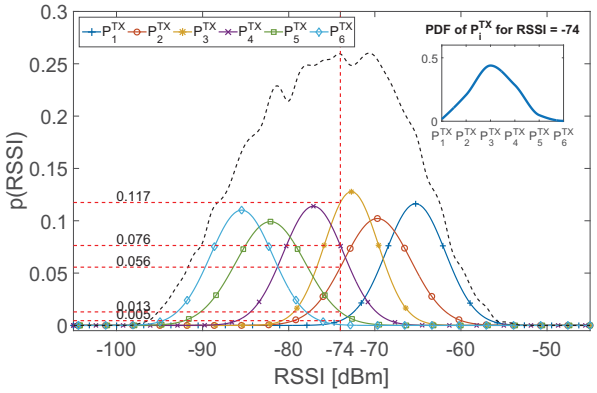


Figure 8: Probability density functions of measured RSSI values per transmission power level.

4.5 Good News and Bad News

In this section, we first utilize the adaptive wormhole mechanism to attack PHYSEC protocols and then show results of our AWOUR protocol using CRKE. We start attacking wormhole detection mechanisms suggested in [23] and CRKE systems. In the latter case, A and B want to agree on a key which is established by using correlated channel profiles. To do so, the first step is to quantize the channel profiles. Then error correction is applied, and later on privacy amplification (hashing). The literature provides a large number of proposals for quantization schemes. We implemented 10 different quantization schemes from the literature, which were recently introduced for CRKE schemes. We additionally implemented three straight forward quantization schemes, using mean, median, and Lloyd-Max thresholds. We analyzed the performance using reciprocal measurements with constant transmission power and compare these with the resulting channel measurements of attacked adaptive wormhole end devices.

The results of the analyses of the quantization schemes are summarized in Table 3. Generally CRKE systems are designed to handle a worst case BER[3] by applying error correction mechanism. Depending on the correction (or detection) capability the maximum BER is given. For example if the code is capable to correct 0.1 bit disagreement the schemes of Tope et al. [37], Aono et al. [5], Mathur et al. [29], Jana et al. [20] (single-bit version), Hamida et al. [14], Wallace et al. [40], and Ambekar et al. [3] are all fully attackable by adaptive wormholes.

Note that Jain et al. [19] applied in his wormhole detection protocol the quantization scheme of Azimi et al. [6] for deriving a bit sequence. The authors utilized classical CRKE for channel-reciprocity verification. Krentz et al.'s [23] detection scheme requires pre-shared secrets for the exchange of measured channel profiles. Then the Pearson correlation coefficient is calculated and a judgement is made. The thresholds for judgement is 0.93. The correlation results demonstrate that the AWOA achieves cross-correlations between 0.86 and 0.96. Therefore, the scheme in [23] is successfully attackable. We achieve false-negative judgment of 22.3%. Jain et al. [19] propose that a BER of ≤ 0.3 concludes the absence of an adversary. The quantization scheme used here gives a BER of 0.0523 with the constant transmission power and a BER of 0.1310 for the adaptive wormhole. Therefore, we achieve false-negative judgement of 100%. Note, the wormhole attack can be easily prevented by increasing the RTT. Therefore, the correlation, mutual information, and efficiency of the system decreases.

The CRKE results using the AWOUR protocol are summarized in Table 3. Due to the low correlation of 0.8 between $-L_1 - L'_2$ and $-L'_1 - L_2$ not all quantization schemes are suitable. Four scheme which are designed to be extremely robust provide BERs lower than 0.05. Those schemes are the ones of Aono et al. [5], Mathur et al. [29], Jana et al. [20], and Ambekar et al. [3].

[3]The *bit error rate* (BER) indicates the percentage of bits that are in disagreement between the initial key material of two parties. BER is evaluated after quantization by the relation: BDR = $\frac{b_e}{b}$ where, b_e is the number of bits in the sequence that disagree and b is the length of the initial key.

Table 3: BER of quantization schemes using Reciprocal Channel (RC) profiles, profiles separated by an AWOA and profiles extracted using AWOUR.

Name	BER_{RC}	BER_{AWOA}	BER_{AWOUR}
Mean th.	0.0482	0.1174	0.1836
Median th.	0.0878	0.2133	0.2427
Lloyd-Max	0.0788	0.1504	0.2883
Tope et al. [37]	0.0019	0.0437	0.1590
Aono et al. [5]	0.0001	0.0046	0.0156
Azimi et al. [6]	**0.0523**	**0.1310**	**0.2258**
Mathur et al. [29]	0.0	0.0076	0.0037
ASBG [20]	0.0	0.0156	0.0481
ASBG-MB [20]	0.0564	0.1203	0.2157
Hamida et al. [14]	0.0920	0.0937	0.4550
Wallace et al. [40]	0.0229	0.0978	0.1967
Patwari et al. [31]	0.0984	0.2335	0.2567
Ambekar et al. [3]	0.0001	0.0033	0.0008

5. RELATED WORK

5.1 Wormholes

Wormholes are realized in different ways. A hidden wormhole is implemented by two nodes which do not participate in the attacked networks. They relay the unchanged traffic between nodes (or networks) which were formerly unreachable. Participating [21] or exposed [23] wormholes are implemented between two legitimate network participants which relay traffic through an out-of-band link.

An established wormhole can be the basis for a number of different other attacks. Tsao et al. [39] discussed sinkhole where the attacker pretends to provide a high-quality route to a communication party and in fact either is not able to forward or knowingly drops all incoming data. As well, Tsao et al. proposed the wormhole as a potential means for selective forwarding attack where the attacker forwards only a subset of the incoming data to all nodes or only forwards incoming data to a subset of all nodes. A wormhole attacker is also able to manipulate selective packages if no further security measures such as encryption and/or authentication is applied. Using wormholes with short lifetime, an attacker is able to run rushing attacks [18] against routing protocols.

To detect or prevent wormholes, multiple schemes were introduced in the past [34, 15, 21, 19, 24]. These techniques can be categorized into three major aspects: (1) Topology, round-trip-time or routing based, (2) hardware-based, and (3) channel(-reciprocity) based countermeasures. For exposed wormholes, Khan et al. [21] introduced a Merkle-tree based wormhole prevention method. Other detection mechanisms which rely on detecting topology or routing anomalies are found in [34, 15]. However, they are either vulnerable to selective forwarding or short wormholes [24]. Chen et al. [11] proposed an approach to detect wormholes using channel measurements and delays. However, this approach may be vulnerable to a low-latency wormhole, e.g., realized by a fast out-of-band connection. Jain et. al [19] proposed a detection mechanism which is based on the reciprocity of RSSI measurements between nodes. As this approach does have issues with false positives and negatives [24], Krentz et al. proposed a scheme called "Secure Channel REciprocity-based WormholE Detection (SCREWED)" which utilizes channel hopping. Both schemes are able to prevent or detect exposed wormholes but are vulnerable to adaptive wormholes.

5.2 Untrusted Relays

Most prior work on key generation with relaying channels considered only trusted relays. However, end-nodes (or their data) often have higher levels of security clearance than the infrastructure, e.g., gateways, routers, and relays. Therefore, the generation of secret keys using untrusted relays is required. He et al. [16] introduced the first PHYSEC key establishment scheme using untrusted relays. To do so, the authors introduced a helper that performs cooperative jamming to establish a secret-key rate larger zero. Unfortunately, jamming capabilities are not provided by today's transceiver modules and, therefore, not considered.

A secret key generation scheme with multiple untrusted relays has been proposed by Lai et al. [25]. The scheme broadcasts the result of the XOR of two keys k_{AR} and k_{RB}, which are generated based on the channels between a relay and two nodes. Both are than able to derive a shared secret key by XORing the broadcast key with their own key. However, to be untrusted the scheme can only work with multiple non-colluding relays, and therefore cannot work with either a single relay or multiple colluding relays.

Thai et al. [35, 36] proposed a novel scheme for generating a secret key between two legitimate nodes and the help of several untrusted relays, all equipped with multiple antennas. The numbers of antennas at the legitimate node should be at least 4, which is not achievable with today's low-resource sensor platforms.

Other approaches were introduced in theory and, further, have serious drawbacks. Our scheme in contrast works with a single untrusted relay (like a central gateway) and low-end sensor devices (such as single-antenna SoC solutions). Furthermore, our proposed scheme is thoroughly evaluated through both theoretical and experimental studies.

6. CONCLUSIONS

In this paper, we demonstrated that AWOAs are real-world threats. We demonstrated on 12 (10 CRKE, 2 AWOA detection) different PHYSEC protocols that RSSI-based systems are vulnerable to AWOAs. The attacks allow the attacker to learn the key or to perform attacks with hidden wormholes. Given the generality of the relay attack, it is likely that CRKE systems based on similar designs, e.g., using amplitude values of CIR or CTF, are also vulnerable to the same attack. We proposed a simple countermeasure that minimizes the risk of AWOAs.

We implemented a testbed based on the IEEE802.15.4 standard, which resembles the real-time capabilities of future 5G network with its short acknowledgement frames (RTT of 1 ms) and narrow bandwidth. We introduced the idea of generating artificial random small-scale fading to ensure that the channel profiles without mean are stationary random processes. We analysed critical coherence time characteristics in order to better quantify the systems' behavior.

Further, the AWOUR protocol for low-end wireless platforms is presented. We demonstrate that fresh key material can be extracted securely over a single untrusted relay. Using state-of-the-art mutual information estimation, we achieve secret-key rates of 0.5 bits per bidirectional communication step. Due to the precise adjustment of the re-

ciprocal channel (and the corresponding random process), the ability to mutually derive key material implies distance bounding. This concept is novel and might have a larger impact in related areas, e.g., remote key-less entry systems or access control in general.

Security and connectivity of low-end platforms are basic requirements for the IoT. The paradigm shift from IoT to the Tactile IoT (TIoT) introduces further constraints such as low-latency communication which make efficient security solutions imperative. We believe that PHYSEC can open up new ways of realizing secure and cheap human tactile and visual feedback control systems.

Future work on this topic may include carrying out more measurements to recheck completeness of the coherence time results. Furthermore, a more formal model description of the introduced protocol is another connecting factor for the future.

7. ACKNOWLEDGMENTS

The authors would like to thank Prof. Dr.-Ing. Kreimeier and Benjamin Fleczok for allowing us to carry out the measurement in their production hall. Many thanks to Jürgen Förster for helping us with the graphics. The authors would also like to thank the anonymous reviewers for the thorough reviews and helpful suggestions.

8. REFERENCES

[1] R. Ahlswede et al. Common randomness in information theory and cryptography. I. Secret sharing. *IEEE_J_IT*, 1993.

[2] S. T. Ali et al. Zero reconciliation secret key generation for body-worn health monitoring devices. In *Conference on Security and Privacy in Wireless and Mobile Networks*, 2012.

[3] A. Ambekar et al. Improving channel reciprocity for effective key management systems. In *Signals, Systems, and Electronics*, 2012.

[4] J. G. Andrews et al. What will 5g be? *IEEE Journal on Selected Areas in Communications*, 2014.

[5] T. Aono et al. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. *Antennas and Propagation*, 2005.

[6] B. Azimi-Sadjadi et al. Robust key generation from signal envelopes in wireless networks. In *Conference on Computer and Communications Security*, 2007.

[7] E. Barker et al. Recommendation for the entropy sources used for random bit generation. *Draft NIST Special Publication*, 2012.

[8] E. Biglieri et al. *MIMO Wireless Communications*. 2010.

[9] M. Bloch et al. *Physical-Layer Security - From Information Theory to Security Engineering*. 2011.

[10] C. Chen et al. Secret key establishment using temporally and spatially correlated wireless channel coefficients. *Mobile Computing*, 2011.

[11] H. Chen et al. On providing wormhole-attack-resistant localization using conflicting sets. *Wireless Communications and Mobile Computing*, 2015.

[12] S. Eberz et al. A practical man-in-the-middle attack on signal-based key generation protocols. In *European Symposium on Research in Computer Security*, 2012.

[13] G. Fettweis. The tactile internet: Applications and challenges. *Vehicular Technology Magazine, IEEE*, 2014.

[14] S. T. B. Hamida et al. An adaptive quantization algorithm for secret key generation using radio channel measurements. In *Conference on New Technologies, Mobility and Security*, 2009.

[15] T. Hayajneh et al. Secure neighborhood creation in wireless ad hoc networks using hop count discrepancies. *MONET*, 2012.

[16] X. He et al. Two-hop secure communication using an untrusted relay: A case for cooperative jamming. In *Global Communications Conference*, 2008.

[17] Y. Hu et al. Wormhole attacks in wireless networks. *Selected Areas in Communications, IEEE*, 2006.

[18] Y.-C. Hu et al. Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. In *Workshop on Wireless Security*, 2003.

[19] S. Jain et al. Wormhole detection using channel characteristics. In *International Conference on Communications, IEEE*, 2012.

[20] S. Jana et al. On the effectiveness of secret key extraction from wireless signal strength in real environments. In *Conference on Mobile Computing and Networking*, 2009.

[21] F. I. Khan et al. Wormhole attack prevention mechanism for RPL based LLN network. In *Ubiquitous and Future Networks*, 2013.

[22] A. Kraskov et al. Estimating mutual information. *Phys. Rev. E*, 2004.

[23] K. Krentz et al. 6lowpan security: Avoiding hidden wormholes using channel reciprocity. In *Workshop on Trustworthy Embedded Devices*, 2014.

[24] K. Krentz and G. Wunder. 6lowpan security: Avoiding hidden wormholes using channel reciprocity. In *Trustworthy Embedded Devices, TrustED*, 2014.

[25] L. Lai et al. Cooperative key generation in wireless networks. *IEEE Journal on Selected Areas in Communications*, 2012.

[26] Z. Li et al. Securing wireless systems via lower layer enforcements. In *Workshop on Wireless security*, 2006.

[27] H. Liu et al. Collaborative secret key extraction leveraging received signal strength in mobile wireless networks. In *IEEE INFOCOM*, 2012.

[28] M. Madiseh et al. Applying Beamforming to Address Temporal Correlation in Wireless Channel Characterization-Based Secret Key Generation. *IEEE_J_IFS*, 2012.

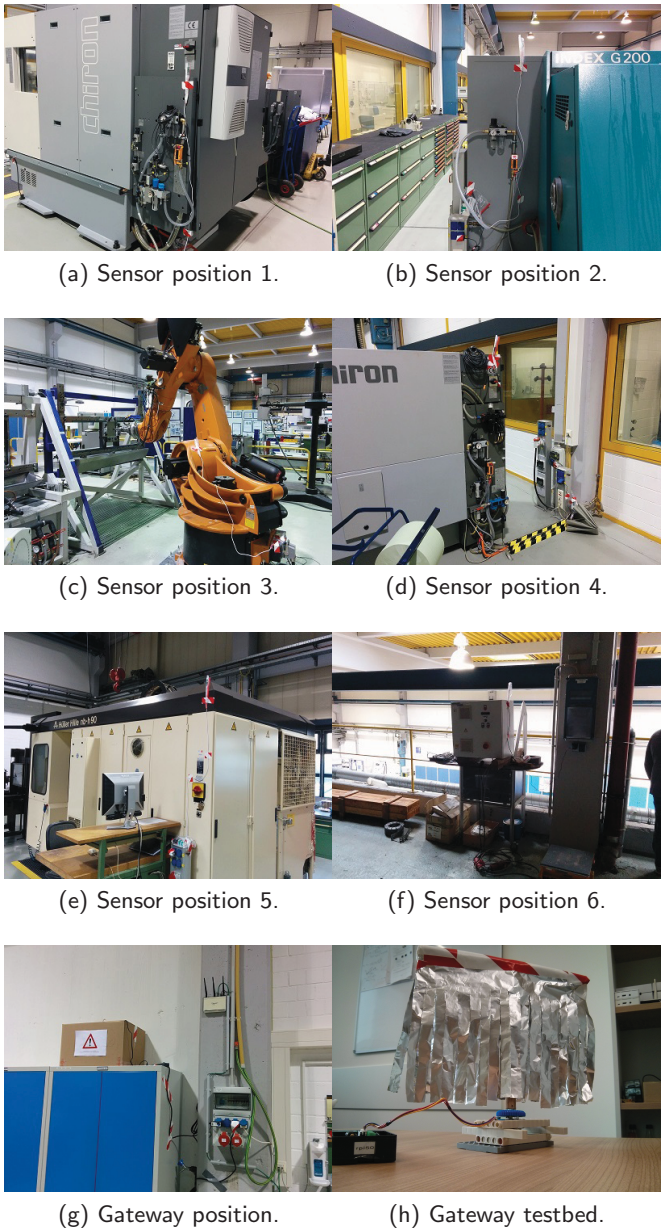
[29] S. Mathur et al. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In *Conference on Mobile Computing and Networking*, 2008.

[30] M. McGuire et al. Bounds on secret key rates in fading channels under practical channel estimation schemes. In *International Conference on Communications, IEEE*, 2014.

[31] N. Patwari et al. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. *IEEE Trans. Mob. Comput.*, 2010.

[32] A. Pierrot et al. Practical limitations of secret-key generation in narrowband wireless environments. *arXiv preprint arXiv:1312.3304*, 2014.
[33] G. S. Smith. A direct derivation of a single-antenna reciprocity relation for the time domain. *Antennas and Propagation*, 2004.
[34] S. Song et al. Statistical wormhole detection for mobile sensor networks. In *ICUFN*, 2012.
[35] C. D. T. Thai et al. Physical-layer secret key generation with untrusted relays. In *IEEE GLOBECOM Workshops*, 2014.
[36] C. D. T. Thai et al. Physical-layer secret key generation with colluding untrusted relays. *Wireless Communications*, 2016.
[37] M. A. Tope et al. Unconditionally secure communications over fading channels. In *Military Communications Conference*, 2001.
[38] W. Trappe et al. Low-energy security: Limits and opportunities in the internet of things. *IEEE Security & Privacy*, 2015.
[39] T. Tsao et al. A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs). Technical report, IETF, 2015.
[40] J. W. Wallace et al. Automatic secret keys from reciprocal MIMO wireless channels: measurement and analysis. *Information Forensics and Security*, 2010.
[41] Q. Wang et al. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. In *Conference on Computer Communications*, 2011.
[42] J. WC Jr. Microwave mobile communications, 1974.
[43] M. Wilhelm et al. Secret keys from entangled sensor motes: implementation and analysis. In *Conference on Wireless Network Security*, 2010.
[44] R. Wilson et al. Channel Identification: Secret Sharing Using Reciprocity in Ultrawideband Channels. *IEEE_J_IFS*, 2007.
[45] C. Ye et al. Information-theoretically secret key generation for fading wireless channels. *Information Forensics and Security*, 2010.
[46] C. T. Zenger et al. A novel key generating architecture for wireless low-resource devices. In *Workshop on Secure Internet of Things*, 2014.
[47] C. T. Zenger et al. Exploiting the physical environment for securing the internet of things. In *New Security Paradigms Workshop*, 2015.
[48] C. T. Zenger et al. On-line entropy estimation for secure information reconciliation. In *Workshop on Wireless Communication Security at the Physical Layer*, 2015.
[49] C. T. Zenger et al. Preventing Relay Attacks and Providing Perfect Forward Secrecy using PHYSEC on 8-bit μC. In *IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia*, 2016.
[50] J. Zhang et al. Mobility assisted secret key generation using wireless link signatures. In *Conference on Computer Communications*, 2010.

9. APPENDIX



(a) Sensor position 1. (b) Sensor position 2.

(c) Sensor position 3. (d) Sensor position 4.

(e) Sensor position 5. (f) Sensor position 6.

(g) Gateway position. (h) Gateway testbed.

Figure 9: The testbeds consisting of six sensors and gateways as well as the aluminum strips based 'random process' generator.