A Novel Key Generating Architecture for Wireless Low-Resource Devices

Christian T. Zenger¹, Markus-Julian Chur¹, Jan-Felix Posielek¹,
Gerhard Wunder², Christof Paar¹

¹ Horst Görtz Institute for IT-Security (HGI), Ruhr-University Bochum, Germany
² Fraunhofer Heinrich Hertz Institute, Germany
{christian.zenger, markus-julian.chur, jan-felix.posielek, christof.paar}@rub.de
gerhard.wunder@hhi.fraunhofer.de

Abstract. Secret key establishment based on parameters of the communication channel is a highly attractive option for many applications that operate in a dynamic mobile environment with peer-to-peer association. On the other hand, high usability and dynamic key management are still very difficult to achieve for wireless devices which have to operate under strict resource constraints. In fact, most previously reported key generation methods cannot operate in such environment. In this work, we present a new system architecture which is suitable also for resource-constrained platforms. Our design strongly focuses on security, rather than a robust key generation rate, as well as on low complexity and efficiency. Our approach has the potential to dramatically reduce the cost of securing small embedded devices for the Internet of Things, and hence make mass production and deployment viable.

Key words: Channel-based key generation, dynamic symmetric keys, online entropy estimation, resource-constrained devices, Internet of Things

1 Introduction

Intelligent and network-compatible everyday objects, which are primarily formed by (small) embedded systems, are coming into the spotlight of economic interest [9]. In recent years, the need for security in resource-constrained systems and Internet of Things (IoT)-systems has grown dramatically [10, 18, 35], e.g., the establishment of secure communication connections for code-updating, function enabling, triggering of actions or transmission of data for Smart Home/Building/Cities, Industry 4.0, Car-to-Car-/Car-to-X-communication, or e-health.

Until now, small embedded systems like sensors or actuators with small \( \mu \)C are secured using (lightweight) symmetric/pre-shared-key cryptography even though these result in inflexible key distribution and management. However, while asymmetric approaches allow greatly improved key management, they result in long (sometimes: unacceptably long) processing time, a large code size,
comparably long messages for key establishment, and considerable energy consumption during encryption and transmission. While there are domain-specific symmetric ciphers, e.g., [6], which are optimized particularly for lightweight, such optimizations are not possible for asymmetric ciphers. Despite almost four decades of research, all known asymmetric algorithms require arithmetic with extremely long operands, as a result the algorithms consume $2 - 3$ times more energy than comparable symmetric primitives [17].

With this work, we address the tension between two critical requirements for IoT. On the one hand, everything, even the tiniest and cheapest platforms that operate under strict resource-constraints, should be securely connected to the Internet without any effort of the user, e.g., manual configuration of keys. On the other hand, overly loose security services, such as key diversity, lead to attacks, such as those illustrated by Eisenbarth et al. [16] and Strobel et al. [38]. Once they recovered the symmetric key, provided to all potential communication partners before deployment, the security posture of the entire system (maybe of the entire product batch) collapses.

Between these two poles we believe that physical layer security (PHYSEC) is a very promising solution for providing security to the IoT. PHYSEC covers most security needs, is considerably cheaper than other solutions, easy to integrate, and provides inherent protection against several important classes of attacks. An amazing fact of PHYSEC is that secret keys are derived out of the physical environment. Therefore, it provides an easy to understand security model for non-experts. It suffices to take care of the spatial environment, since security can be assumed if no other device is within a certain security radius. A possible successful passive attack would require an antenna set-up within a specific security radius aligned to each device separately.

1.1 Channel-Based Key Establishment: Principles and Preliminaries

PHYSEC introduced by Hershey et al. [24] is a new paradigm for generating shared secret keys. The approach is based on a common estimation of the wireless transmission channel by the sender and receiver, whereby the secret key will be derived from channel parameters and relies on the principle of channel reciprocity [37]. Specifically, this means that the channel from Alice to Bob is the same as the channel from Bob to Alice. The reciprocity of practical channels between two nodes is usually sufficiently high, as well as its entropy of spatial, temporal, and spectral characteristics.

Besides common randomness, the scheme is also inherently secure against attacks. If an attacker’s distance to both legitimate nodes is high enough, the channel parameter he observes to each node is uncorrelated and a passive attack is not possible. In real environments this fact is often given, if the distance is
greater than about a half of the carrier wavelength $\lambda$. For systems working at 2.4 GHz the distance $l_c$ is 62.5 mm. Channel reciprocity and spatial correlation are the key properties of channel-based key generation protocols. These concepts have been validated by a large campaign of measurements [39, 2, 3, 27, 31, 40, 30, 20, 1].

1.2 Related Work

Several early research and development efforts in key generation systems based on channel gains$^1$ have addressed robust key generation, e.g., [39, 2, 28, 41, 3, 30, 27, 40, 31, 8, 20, 1]. For the sake of simplicity, we split the key generation systems into roughly three functional elements: quantization of channel estimations, information reconciliation of Alice’s and Bob’s quantizes channel estimations, and the handling of its temporal decorrelation.

**Quantization:** Based on [24], Tope et al. [39] introduced 2001 the very first channel-based key generation protocol. They suggested a *lossy* quantization scheme based on two thresholds $\gamma_+$ and $\gamma_-$ for converting channel measurements $x$ into random key bits $Q$ such that $Q(x) = 1$ if $x > \gamma_+$ and $Q(x) = 0$ if $x < \gamma_-$. Otherwise $x$ is dropped. Here, $x$ denotes the sample value, and $\gamma_+$ and $\gamma_-$ denote the upper and lower thresholds, respectively. Tope et al. defined $\gamma_+$ and $\gamma_-$ as fixed system parameters. Consequently, several schemes were proposed using different rules to determine the thresholds and selecting samples [2, 27, 30]. Note that such threshold techniques make the system artificially robust against noise etc. but have serious security issues as deductively shown by Eberz et al. [15]. Their passive attack is based on receiving correlated channel estimations. Wallace et al. [40] introduces an interesting entropy maximizing and noise reducing quantization technique. Unfortunately, their algorithm is very computationally intensive. Additionally, these and further schemes require exchange of data for quantization, e.g., [3, 31, 1]. Note that communication consumes a significant amount of energy that would shorten the life time of a low-resource device. For the same reason we do not consider approaches based on jamming techniques, e.g., [20]. By contrast, in this work we adapt the scheme of Ye et al. [41], presenting a *lossless* multiple bit quantization scheme based on unit-variance Gaussian distribution input sequences and an equiprobable output.

**Information Reconciliation:** Information reconciliation can be done using various error correcting codes [29, 11, 33] and a public channel as presented by Brassard et al. [7]. Their protocol called CASCADE realizes error correction

---

$^1$ Because the channel gain can be measured more easily than time delay or phase and it is provided by virtually every wireless communication chip, we are focusing on channel gain techniques.
on the basis of exchanging parity check bits. After CASCADE has been published, a number of works have improved the algorithm and reduced the information leaked. For instance, Zhang et al. [43] realized information reconciliation by applying RS-codes. Since the exchange of parity check bits occurs over the public channel, they disclose Eve information about the key material and reduce the efficiency of the scheme. In our opinion multiple leaks, e.g., through a correlated channel estimation and parity check bits, could lead to an uncontrollable security system. Aono et al. [2] suggest a very interesting solution. To ensure secret key agreement, an algorithm is performed transmitting the syndrome from binary codes. For this reason, no information of the key material will be revealed. Dodis et al. [13, 14] present formal definitions and efficient techniques for turning noisy information between two parties into secret keys.

**Decorrelation:** Because a single channel estimation usually does not provide enough entropy for a symmetric key, e.g., for a 128 bit security level, multiple channel estimation over time are considered. As discussed by Patwari et al. [31], multiple channel estimation over time can contain correlated components, which makes it hard to verify the security level of the key material. As a result, recent approaches were confined to utilize only a portion of the quantized channel profile by downsampling the raw measurements in time to reduce strong correlations. However, this could reduce the rate of key extraction. Previous work [31, 12] proposed an alternative to downsampling, the discrete Karhunen-Loève transform, to convert the channel measurements into uncorrelated components. Chen et al. [8] proposed an similar complex approach based on large covariance matrices. This approach is of significantly higher computational complexity than the downsampling approach and not feasible on resource-constrained devices in our opinion.

**Summary:** Recent publications do not specifically address the applicability of PHYSEC for resource-constraint IoT platforms. The main challenge is that such tiny IoT platforms forbid the use of heavy cryptographic or signal-processing techniques with high energy consumption. Equally important is the impact of recent attacks for choosing system components, e.g., the quantization scheme.

### 1.3 Contributions

In this paper we present and evaluate a complete key generation architecture for establishing symmetric keys out of the common wireless channel. Our system is strongly designed for resource-constrained platforms and achieves strong security instead of "robustness only", where previous publications have focused on. As the main contribution of this work, we extract and discuss in detail a novel system architecture which contains known as well as new ideas which all serve our specific purpose. The following main contribution will be discussed:
Existing approaches require mobile devices or significant movement in the environment as the main generator of common secret material [32]. In real environment, motion is not constantly given. As a result, existing approaches do not just stop working, they create false-positive agreed key material. This material gets collected and post-processed with the effect of restarting the protocol over and over again, thus stressing the battery. We propose a solution, that is based on the detection strength rather than on the correction strength of well-known error detection techniques.

Another key element of our work is a novel solution of handling memory-afflicted random sources that simultaneously reduce the complexity of one of the two key generation participants. We utilizes an online entropy estimation as an alternative to applying expansive decorrelation techniques by both participants, as suggested by recent publications [31, 12, 8]. Our system utilize the online entropy estimation techniques of the NIST draft [4] for creating a load-balance to the advantage of a resource-constrained device. Until now, no system architecture introduces approaches for online entropy estimation or at least online statistical testing. In our opinion, such a monitoring technique is an important element of channel-based key generation systems. However, as a result of our modular system architecture structure, our monitoring technique as well as the information reconciliation technique can easily be added into recent approaches.

2 Adversarial Model

In wireless networks, most attacks can be classified into two categories: passive and active [36]. Traffic analysis and eavesdropping belong to the class of passive attacks. In channel-based key generation systems, we differentiate between the eavesdropping of channel estimations or of data transmissions. The passive attacker Eve is able to get the exact transmitted data, whereby the channel estimation she receives is only a correlated version of Alice’s and Bob’s. In this scenario, the most potent attacker (with the strongest correlation) is the one with the shortest distance to Alice and/or Bob. We do not consider Denial-of-Service attacks, hardware modification or man-in-the-middle/masquerade attacks [36]. We do not address advanced approaches for the authentication of the legitimate users (Alice and/or Bob). By way of example, we like to refer to the push-button-connect authentication method of the Wi-Fi Protected Setup (WPS) as user-friendly and a widely used method.

3 Novel Security Architecture for Resource-Constrained Devices

In the following, we describe the design of a complete channel-based key generation protocol for resource-constrained devices that operate in a dynamic mobile
environment with peer-to-peer association. An overview of our system architecture is given in Fig. 1. The central system between channel estimation and the symmetric encryption scheme is the technique turning the correlated data into a symmetric key, without revealing any information unintended.

Fig. 1. Overview of the components involved in the security architecture for resource-constrained devices: Extracting secret keys from variations of the channel. Grey blocks are optional blocks.

The channel estimation block represents the randomness extractor, for instance by measuring the impulse response of the wireless channel. An alternative could be the received signal strength (RSS). Both Alice and Bob convert their channel estimations into symmetric key bits using quantization. Bob can be considered as an low-resource device. The carefully chosen information reconciliation technique corrects bit errors of the quantized channel estimations between Alice and Bob. A random number generator is a critical component in every cryptographic device. Therefore, an important security feature of the entire system design is a statistical test to provide online entropy testing. For this purpose we introduce two different statistical testing blocks: the online entropy estimation block and the optional health testing block. With the estimated entropy, the synchronized key material can be quantified and the health/total breakdown test can be considered to reduce the amount of data for further blocks. In conclusion, the privacy amplification block collects entropy to generate a secret key as long as it takes to achieve a predefined security level.

2 Note, RSS are provided anyway by almost every wireless communication chip during reception of data. Unfortunately, they do not entirely fulfill the security related properties. As a result the spatial decorrelation, introduced in Section 1.1, is not guaranteed.
3.1 Problems of Common Channel Estimations for Security Systems

A wireless channel between two parties can be estimated by exchanging a known pseudo noise signal. The received signal is affected by various phenomena, which characterize the channel. Doing so in both direction within the so called coherence time \cite{19}, we call common channel estimation. We now describe a realistic channel estimation scenario as well as three problems of utilizing a common entropy source based on wireless radio channels.

For generating a symmetric key based on a common channel, so far several mutual transmissions between two nodes are required. Several transmissions for gaining a symmetric key stay in conflict with an energy efficient solution for resource-constrained platforms. Interestingly, during usual (application) data transmission channel estimation can be performed on the fly. We call this recycling-based channel estimation. For instance, some IEEE 802.11 Wi-Fi standards already uses a 13 bit Barker sequences for package synchronization. Such sequences are perfectly applicable for estimating wireless channels \cite{19}. However, when utilizing reciprocal channel estimations as a random variable for key generation the following problems have to be considered:

**Problem 1:** Probability density functions of channel estimations are usually *not uniformly distributed*. As a result, the key material is partially predictable. Additionally, this distribution function can be time variant, e.g., depending on changing environments. We present our solution in Section 3.2.

**Problem 2:** Alice’s and Bob’s channel estimations are (highly) correlated, but usually not perfectly equal over time. Potential failure sources in reciprocal channel estimations are: bad synchronization, noise, nonlinearity, and too rapid movement. These lead to a need of error handling, which always strengthens an attacker, as we discuss in Section 3.2 and 3.3.

**Problem 3:** The channel coefficients of the reciprocal channel estimations (Alice to Bob and vice versa) may be *memory-afflicted*. This happens if the sampling rate \( r_s \) of the channel coefficients is higher compared to the inverse of the coherence time \( T_c^{-1} \) \cite{19}. We present and discuss our solution in Section 3.4.

3.2 Efficient Entropy Maximizing Quantization

For quantization of the channel estimation we implement a low-complex quantization scheme with multiple bit and equiprobable output. The symbol mapping is chosen according to the input distribution, as introduced by Ye et al. \cite{41}. The quantization algorithm works with blocks of the length \( 2^l \) bit. The algorithm first sorts the values (together with its initial position) by value size. Then it replaces the values by the corresponding \( n \) bit Gray-code \cite{21} and finally sorts it back. This can enhance the randomness of the pre-key material. Our scheme
differs from Ye’s approach by being independent of specific probability density functions of the channel measurements. Therefore, our secret key generation algorithm is also not limited to the input of any specific channel state information representation, e.g., RSS, channel phase, or complex-valued channel profiles.

For evaluation we use a fair comparison techniques as well as the metrics Bit Disagreement Rate (BDR) and Initial Key Generation Rate (IKGR) as introduced by Guillaume et al. [22]. For visualizing of the robustness of quantization schemes, Fig. 2 (a) illustrates the BDR course of Mathur et al. [30], Jana et al. [27], and our scheme as a function of the Pearson correlation coefficient $\rho$. Fig. 2 (b) illustrates the IKGR of Mathur et al. [30] over $\rho$. Our scheme is lossless, therefore the IKGR depends only on the $n$ bit output symbol. The correlation coefficient implicates the distance between two parties [26]. The BDR course of Mathur’s and Jana’s quantizer does not have a high slope, what makes it invulnerable by an (close located) eavesdropper. For instance, given are the correlation coefficients of Alice-Bob’s channel estimations with 0.97 and Eve-Bob’s with 0.8. Applying Mathur’s scheme, the BDR between Eve’s and Alice’s pre-key-material would be only 0.06. Thereby, our scheme would provide a difference of the BDR of 0.45. This is a great security feature because less correlated observations do not lead to the same key material, which makes our scheme not vulnerable against the attack of Eberz et al. [15].

3.3 Information Reconciliation

According to the reciprocity principle, the generated bit strings are theoretically identical. However, there exist discrepancies due to missing channel dynamics$^3$.

$^3$ In dynamic scenarios where the two devices are mobile, and/or where there is a significant movement in the environment, high entropy bits are obtained fairly quickly [32].
half-duplex transmission and estimation errors caused by hardware variations, interference and noise. For reconciliation, we apply the BCH syndrome decoding approach introduced by Dodis et al. [13], which is an efficient secure sketch. The algorithm interprets quantizer’s output bit string as code words. Therefore, the processing is carried out on a block basis of length $n$. For any pre-key material block/received word $y_b = x + e_b$ of Bob and $y_a = x + e_a + e_b$ of Alice, the corresponding syndromes $\text{syn}(y) = y \cdot H$ of the length $n - k$ can be easily calculated. $H$ is the $n \times (n - k)$ parity check matrix of a $(n,k,d_{\text{min}})$ linear block code and $x$ is the underlying code word. The resource-constrained device, represented by Bob, sends its syndrome $\text{syn}(y_b)$ to Alice. She calculates $\text{syn}(e_a) = \text{syn}(y_a) - \text{syn}(y_b)$ and calculates by applying decoding techniques the error $e_a$, which can be very computationally intensive. After that she calculates $y_b = y_a - e_a$ and checks the validity of $\text{syn}(y_b) = \text{syn}(y_a - e_a)$. Important to mention is that, compared to other schemes, the public information $\text{syn}(y_b)$ is only dependent on the error, instead of the information. Therefore, the number of effective bits is decreased only by the $n - k$ syndrome bits [2].

As stated before, our quantization scheme is very susceptible against low reciprocity. The disadvantage of this security feature is that only parts of the channel estimation with very high reciprocity lead to key material, everything else leads to a high BDR. This in turn leads to false-positive validations of $\text{syn}(y_b) = \text{syn}(y_a - e_a)$ and then the protocol have to start all over again. We address this problem by utilizing, beside the correction strength, the detection strength as well. For performance evaluation we apply small BCH($n, k, d_{\text{min}}$) codes with $n \leq 63$. The corresponding detection-, correction-, and code rates are $(d_{\text{min}} - 1)/n$, $t/n$, and $k/n$. This behavior is exemplarily illustrated in Fig. 3(a) for all codes with $n = 63$. The error detection region (yellow) can be seen as
a BER guard interval. Fig. 3(b) illustrates the correlation coefficient on a block basis of a real-world measurement and its relation to a BCH(67, 7, 15) code. As demonstrated in Section 3.2, only channel estimations with high reciprocity provide high security. Applying the combination of the introduced quantizer as well as the error correction scheme, a selection of high reciprocal channel estimation sequences is possible, without strengthening a passive eavesdropper.

3.4 Online Entropy Estimation for Load-Balancing

As previously stated, there is no guarantee that multiple channel profiles are absolutely independent across time. Furthermore if a single channel profile contains multiple components (in time or frequency), then the same assumption holds for the different components. Recent publications suggest the execution of decorrelation techniques by both Alice and Bob [31, 12, 8]. In our opinion, such calculations are unacceptable expensive for low-resource devices.

Therefore, we searched for a solution where one of the two participants has low or no costs. Our approach handles memory-afflicted random sources by guessing the entropy of its output. We apply the entropy estimation after information reconciliation. The reason for that is that at this point both participants received synchronized symmetric key material, which is not afflicted anymore by useless entropy coming from noise, instead of from the reciprocal channel. The entropy estimation for not independent and identically distributed random variables as demonstrated in the draft 800−90B of NIST [4] matches perfectly to our application. The draft recommends the five tests: collision test, partial collection test, Markov test, compression test, and frequency test. The estimation works on a per sample basis. Therefore, the output bit size of the quantizer is an important parameter for entropy estimation. Given fixed length input block, each test provides an estimation of its entropy, whereby the smallest value is used as the final result. The length must be chosen by considering the maximum possible memory of the channel.

The main idea here is the fact that we can handle quantized channel data including redundancy by creating a load-balance to the advantage of a resource-constrained device. The entropy estimation might be done only by one of the two participants. For instance, only by a central gateway with permanent power supply. Our solution represents an alternative to the heavy calculation of decorrelation techniques on both sides.

Total Break Down-/Healthy Test: Motivated to reduce the energy consumption, especially for mobile devices, we introduce an optional online statistical test. The idea is to reject low entropy data blocks that do not pass this test and therefore prevent further computations. We exemplary suggest the 256-bit wide online health check unit of Intel’s Ivy Bridge random number generator [23].
3.5 Privacy Amplification

Uniformly distributed and precisely reproducible random strings are the initial requirement for cryptographic secrets. If those requirements are not fulfilled for a random variable, privacy amplification is required [25]. Moreover, during the reconciliation phase the eavesdropper will also have access to the error correcting bits. To avoid possibilities of key predictions and to collect entropy out of the initial key material, we apply a universal hash function for privacy amplification (e.g., SHA-2 [34], SHA-3 [5]).

4 Prototype Implementation and Results

In this work, we present the implementation results of a prototype system based on the hardware platform Raspberry Pi. It is a cheap credit-card-sized computer that is universally deployable with a Linux-based operating system and flexible expansion options. We utilize the computer together with a TP-Link TL-WN722N Wireless USB Adapter as a universal IoT device. We evaluate a series of measurements using the experiment plan shown in Fig. 4. The experiment consists of three nodes (Alice-Bob-Eve). Two nodes (Bob-Eve) are stationary and one node (Alice) is moving as illustrated in Figure 5.

Network traffic is generated by an independent application (simulating sensor data). Our prototype implementation utilize the channel estimation provided by those transactions. Therefore, we choose Wi-Fi chips providing the MAC-layer in software. We manipulate this driver-software in a way that they can still work as usual, by providing the RSS as well as a micro-counter of each IEEE 802.11 frames. Because of unbalanced up- and down-link traffic we sequently synchronize the temporal measurements.

We implemented the hole system as introduced before. Additional to our quantization scheme, we implemented and analyzed the schemes from Mathur et al. [30], Jana et al. [27], and Ambekar et al. [1] as well. For the evaluation we present a measurement session, that consists of 50,000 RSS values measured with a rate of 90 samples per second using IEEE 802.11 conform frames between Alice and Bob. As shown in Figure 6, the experiment channel estimations obtain a high reciprocity between Alice and Bob of $\rho \approx 0.99$ (measured with the Pearson correlation coefficient as shown by Guillaume et al. [22]), as well as between Alice and Eve of $\rho \approx 0.85$. The results of the quantization schemes are reflected in the BDR column of Table 1. The table shows that the error rate varies considerably across the quantization schemes; the higher the robustness of the scheme, the lower its error rate. The classical KGR as known from literature is reflected in the $\text{KGR}_{IR}$ column. Here, the highest rate of our
scheme is 2.5 bps. Our rate is relatively low when comparing it to the rates of other schemes, e.g., Ambekar et al. [1] with 14.7 bps. After weighing the bits with its estimated amount of entropy, our scheme achieves the best result for the ratio $\frac{\text{KGR}_{IR}}{\text{KGR}_{H(X)}}$, but not the best performance. However, even if our scheme does not provide the best performance, it is able to generate key material based on a security motivated architecture. Additionally, let us recall the fact that our quantization scheme does not require communication.

Table 1. Detailed evaluation results of the channel-based key establishment scheme by applying different quantization schemes of the literature.

<table>
<thead>
<tr>
<th>Quantizer</th>
<th>$\text{BDR}_{AE}$</th>
<th>$\text{BDR}_{AE}$</th>
<th>$\text{KGR}^{\text{ip-rate}}$</th>
<th>$\text{det-rate}$</th>
<th>$\text{cor-rate}$</th>
<th>$\text{KGR}_{H(x)}$</th>
<th>$H_{ext}(x)$</th>
<th>$\text{KGR}_{H(X)}$</th>
<th>$\text{BER}_{AE}^{\text{IR}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jana ASBG [27]</td>
<td>0.0261</td>
<td>0.4801</td>
<td>55.4</td>
<td>0.0000</td>
<td>0.0290</td>
<td>0.9710</td>
<td>5.9774</td>
<td>0.0088</td>
<td>0.0526</td>
</tr>
<tr>
<td>Jana [27]</td>
<td>0.1657</td>
<td>0.4738</td>
<td>182.0</td>
<td>0.0050</td>
<td>0.1808</td>
<td>0.8141</td>
<td>16.4632</td>
<td>0.1001</td>
<td>1.6474</td>
</tr>
<tr>
<td>Ambekar [1]</td>
<td>0.1992</td>
<td>0.4824</td>
<td>182.0</td>
<td>0.0126</td>
<td>0.2596</td>
<td>0.7278</td>
<td>14.7175</td>
<td>0.1292</td>
<td>1.9020</td>
</tr>
<tr>
<td>Aono [2]</td>
<td>0.1255</td>
<td>0.4841</td>
<td>68.3</td>
<td>0.0017</td>
<td>0.0958</td>
<td>0.9025</td>
<td>6.8441</td>
<td>0.0927</td>
<td>0.6344</td>
</tr>
<tr>
<td>Mathur [30]</td>
<td>0.0129</td>
<td>0.4852</td>
<td>4.9</td>
<td>0.0000</td>
<td>0.0000</td>
<td>1.0000</td>
<td>2.3435</td>
<td>0.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>Modified Ye [42]</td>
<td>0.3281</td>
<td>0.4726</td>
<td>91.0</td>
<td>0.0404</td>
<td>0.7146</td>
<td>0.2449</td>
<td>2.4767</td>
<td>0.1851</td>
<td>0.4584</td>
</tr>
</tbody>
</table>

5 Conclusions and Future Directions

This paper addresses the problem of inflexible key distribution and management for applications that operate under strict resource constraints in a dynamic mobile environment with peer-to-peer association. The main challenge is the fact that such platforms forbid the use of heavy cryptographic or signal-processing techniques with high energy consumption. We presented the design and the evaluation results of a channel-based key generation architecture that fulfilled these objectives. It is based on recycling channel estimations, utilizes a security-only quantization scheme combined with an efficient information reconciliation scheme. The main difference to similar publications is our novel approach to handle memory-afflicted channel measurements. In addition, by addressing low-resource platform, the method allows load-balancing between both nodes.

As the results of our simulation show, we are able to build and scale a physical-layer security protocol for the IoT. The full protocol runs on our real-world devices related test hardware. The protocol itself is detached from the necessary driver modification and may run on the application-layer of many systems. The driver currently needs to be open source and the capability of receiving RSS on a per frame basis, as described in IEEE 802.11, to be efficient.

Currently, we are working on several software and hardware realizations for confirming the practicality regarding energy and resource efficiency, as well as on advanced adversary models and security analysis.
Acknowledgments

This work was supported in part by the German Federal Ministry for Education and Research within the project Providing Physical Layer Security for the Internet of Things (PROPHYLAXE) (Grant 16KIS0005 and 16KIS0010). Many thanks to Hasan Tekin and Johannes von Reth for creating and editing figures; the members of the EMSEC Group, and the PROPHYLAXE team for feedback on drafts.

References


**Appendix:**

Figure 4 shows one of three Raspberry Pis we use in our real-world related experiments. The floor plan in Figure 5 illustrates the arrangement of the Raspberry Pis in our building. The multiple antenna positions of Alice represent the movement of the device. The affects of movement can be seen in Figure 6. The signals of Alice and Bob seen in Figure 6(a) are highly correlated, which is not the case for Eve. Multiple samples blocks of Alice, Bob, and Eve differ in correlation strength. This can be seen in Figure 6(b) for 800 subsequent sample blocks. This also illustrates Eve’s possibility of getting single high correlated blocks, but these are never as correlated as blocks of Alice and Bob.
Fig. 4. The prototype platform: Raspberry Pi Model B.

Fig. 5. The layout of the experimental setup.

Fig. 6. Successive channel estimates of the process by Alice, Bob and Eve (a) as well as the correlation coefficient over time (b).