Effects of Channel Characteristics and Design Parameters on Secret Key Generation Rates

Amitha Mayya[1], Miroslav Mitev[1], Arsenia Chorti[1,2], Gerhard Fettweis[1]
[1]Barkhausen Institut, Dresden, Germany
[2]ETIS UMR 8051, ENSEA, France
{amitha.mayya, miroslav.mitev, arsenia.chorti, gerhard.fettweis}@barkhauseninstitut.org

***Abstract*—In this work we provide experimental results of a secret key generation (SKG) protocol using filterbanks to obtain observations of a frequency modulation continuous waveform. To distil the channel randomness, our approach relies on exchanging linear complex chirp signals over a large bandwidth, as is customary in radar systems. Our experiments shed light on how the key generation rates depend on both the channel characteristics (line-of-sight (LoS), non-line-of-sight (NLoS), dynamic, static) as well as the choice of system parameters used in the different stages of the protocol. Furthermore, we consider the presence of passive eavesdroppers and evaluate the information leakage.**

I. Introduction

Security is a serious concern when it comes to 6G. The emergence of quantum computing makes existing public key encryption algorithms insecure [1]. In this regard, SKG using physical layer security (PLS) can be considered as a promising lightweight alternative where shared randomness is extracted directly from the wireless channel. The SKG protocol consists of four steps: randomness extraction, quantization, information reconciliation and privacy amplification. The protocol allows two nodes to extract a shared secret.

In this work, the shared random component of the reciprocal channel is extracted from channel power observations using a filterbank technique to measure received signal strength of frequency modulation continuous waveform (FMCW) signals. Each party converted the power observations to information bits using a library of available quantizers. We note that a main advantages of the filterbank approach is that it can be used with any arbitrary waveform and eliminates the need to have matched receivers (assuming the transmit power spectral density (PSD) is known). Due to the noise in the channel and imperfect channel estimation, the two observations differed. This was corrected during the information reconciliation step using distributed source coding techniques. Finally, during privacy amplification, potential information leakage (that may have occurred in the previous steps) was compressed. The leakage was measured using a conditional min-entropy estimator which gave an estimation of the number of unpredictable, random bits. On these bits, compression was performed using one-way collision resistant function such as a cryptographic hash function.

In this work we aimed at answering the following question. *How the channel characteristics and design parameters affect the SKG rates?*. To answer this question we performed a measurement campaign in a set of different scenarios and investigated the SKG rates achievable in all scenarios under different system parameters. We note that this work is a practical validation of our previously published analytical and simulation results [2], [3].

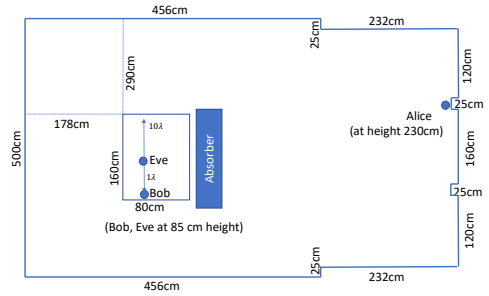

Fig. 1. Measurement Setup

II. System model

For our experiment, we configured three USRP-2974s, each with single antenna, as two legitimate users, Alice and Bob and an eavesdropper, Eve. Fig.1 shows the real-life measurement setup. Experiments were performed in 4 scenarios, namely LoS static, LoS dynamic, NLoS static and NLoS dynamic. Dynamic scenarios are realized through movements of objects and people in the room. Static channel measurements were realized during the nighttime and the channel remains static. The LoS and NLoS scenarios were created by the absence or presence of absorbers between the antennas of Alice and Bob. Alice and Bob transmitted complex chirp signals in a time division duplex (TDD) manner. Ten different positions were considered for Eve, ranging from 1λ to 10λ distance w.r.t. Bob position. As a passive eavesdropper, Eve constantly listened to the exchange between Alice and Bob. For the considered passband frequency, $f_c = 3.75$GHz, the wavelength $\lambda \approx 8$cm. In this setup we exchanged 10^5 chirp signals at each positions of Eve. The signal bandwidth is $B = 70$MHz, the sampling rate was $f_s = 140$MHz and the symbol duration was $T_s = 17.1875\mu$s. We measured the received signals at Alice, Bob and Eve to implement the SKG protocol detailed in the next sections to obtain the secret key and evaluate the SKG rates in all different environments.

A. SKG protocol

1) Randomness extraction: The received signals at Alice, Bob and Eve can be represented as

$$y_l(t) = x(t) * h_l(t) + w_l(t), \tag{1}$$

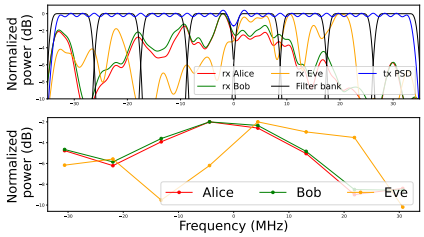

Fig. 2. PSDs of transmit signal and receive signals (Alice, Bob and Eve) and filterbank (upper) and the time averaged power measurements of Alice, Bob and Eve (lower) for 8 filters

where $l \in \{A, B, E\}$ stands for Alice, Bob and Eve, respectively, $x(t)$ is the transmit signal, $w_l(t)$ is an AWGN variable. The channel impulse response can be written as [4],

$$h(t) = \sum_{n=1}^{N} \alpha_n(t) e^{-i\phi_n(t)} \delta(\tau - \tau_n(t)). \tag{2}$$

Due to reciprocity, between Alice and Bob, $h_A(t) \approx h_B(t)$. Here $\alpha_n(t)$ is amplitude attenuation, $e^{-i\phi_n(t)}$ is the phase shift and $\tau_n(t)$ is the time delay of the n^{th} multi path component (MPC), N is the total number of MPCs. The received signals were filtered frame wise using a filterbank consisting of K band pass filters and the averaged power at each of the frequency band was measured:

$$P_l = [\hat{p}_{l,1}, \hat{p}_{l,2} ... \hat{p}_{l,K}], \tag{3}$$

where $\hat{p}_{l,i}$ was the average power of at a given frequency given by $\overline{|g_k(t) * y(t)|^2}$. The operator $\overline{(\cdot)}$ denotes time averaging and $g_k(t)$, $k = 1, \ldots, K$, is the prototyping bandpass filter with center frequency $-\frac{B(K-2j+1)}{2K}$. The filterbank was constructed of K raised cosine filters each with bandwidth B/K and roll-off 0.25. Fig. 2 illustrates the PSD of transmit signal and received signals at Alice, Bob and Eve measured using Welch's method. The time averaged power measurements were denoted by the dots for each frequency band. Channel correlations between Alice and Bob result in similar power measurement for each frequency band while that of Eve was noticed to be different.

2) Quantization: The power measurements were quantized into binary information bits. We defined a grey coding scheme, where number of bits per power measurement equals to $\log_2(Q)$ where Q is the number of quantization levels. As illustrated in Fig. 3, two quantization approaches were considered: a linear quantizer where the quantization regions were defined by evenly dividing the frame power measurement range into Q levels; a cumulative distribution (cdf) quantizer where the quantization was defined by computing the inverse of the cdf for each of the quantile regions [5]. Fig. 3 shows an example of both methods using 8 quantization levels. The obtained binary sequence at the end of this step was of length $r_l \in \{0,1\}^{Klog_2Q}$ for K filters and Q quantization levels.

3) Information reconciliation: To perform this step we used Slepian-Wolf based error correction. To correct errors one of the users (Alice) sent a syndrome s_A over a public channel. The second user (Bob) used this information to correct errors using an ECC decoder. In this work information reconciliation was performed using Polar codes.

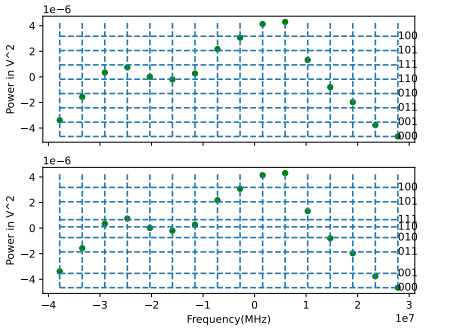

Fig. 3. Quantization thresholds and grey codes per level for linear (upper) and cdf based (lower) quantizers with 8 levels (3 bits per level)

4) Privacy amplification: The conditional min-entropy of an observation is a conservative measure of the amount of secrecy. It estimates the number of secure bits in the observations of Alice (Bob) conditioned on the observations at Eve. The information leakage was measured as [6]

$$\text{Leakage} = H_\infty(r_A) - H_\infty(r_A|r_E, s_A), \tag{4}$$

where $H_\infty(r_A)$ is the min-entropy of Alice and $H_\infty(r_A|r_E, s_A)$ was the conditional min-entropy of Alice w.r.t Eve's observations and the syndrome leaked during the information reconciliation step. To ensure confidentiality, the key at the output of the SKG protocol should be of size $|k| \leq H_\infty(r_A|r_E, s_A)$.

III. Discussion

In this poster we present experimental results on how different channel conditions and system parameters (number of filter, quantization type, quantization levels, code rate) affect the performance of the SKG protocol. Furthermore, we evaluate the leakage to nearby eavesdroppers in real-life setups.

Acknowledgment

Hexa-X-II project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101095759.

References

[1] L. Mucchi, S. Jayousi, S. Caputo, E. Panayirci, S. Shahabuddin, J. Bechtold, I. Morales, R.-A. Stoica, G. Abreu, and H. Haas, "Physical-layer security in 6g networks," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1901–1914, 2021.

[2] M. Mitev, A. N. Barreto, T. M. Pham, and G. Fettweis, "Secret key generation rates over frequency selective channels," in *IEEE Veh. Tech. Conf. (VTC-Spring)*, 2022, pp. 1–5.

[3] M. Mitev, A. N. Barreto, T. M. Pham, M. Matthé, and G. Fettweis, "Filterbank secret key generation rates in multipath channels," in *IEEE Global Commun. Conf. (GLOBECOM)*, 2022.

[4] A. Goldsmith, *Wireless Communications*. USA: Cambridge University Press, 2005.

[5] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, 2010.

[6] G. Smith, "On the foundations of quantitative information flow," 03 2009, pp. 288–302.