Practical Secret-Key Generation by Full-Duplex Nodes with Residual Self-Interference

Hendrik Vogt, Kevin Ramm, Aydin Sezgin
Department of Electrical Engineering and Information Technology
Ruhr-Universität Bochum, Germany
{hendrik.vogt, kevin.ramm, aydin.sezgin}@rub.de

Abstract—**In the upcoming Internet of Things (IoT), encryption of confidential data by *secret keys* is vital. Secret-key generation from *reciprocal* wireless channels has received much attention in the research community in recent time. However, most implementations were restricted to half-duplex channel probing only. Communication setups with full-duplex (FD) capability enable new prospects for secret-key generation, since the inherent superposition of FD signals renders the acquisition of secret information more difficult for an eavesdropper. In this work, we demonstrate a practical testbed with FD capability in order to evaluate its advantages for secret-key agreement. We quantify the performance by computing correlation coefficients and mutual information of all channel estimates. Our work provides new insights into the opportunity of *downgrading* the capabilities of eavesdroppers by using full-duplex nodes.**

I. Introduction

Modern cryptography heavily relies on the availability of secret keys, since encryption of confidential messages is only applicable if the legitimate users have access to a shared secret. However, the secure *distribution* of such keys among the users is a challenging task, especially if the number of devices is huge, as expected in future "Internet of Things" (IoT) environments. Generally, a conventional public-key infrastructure (PKI) is expensive to maintain. In order to tackle that problem, properties of the physical environment can be be exploited as a source of common randomness. Wireless channels deliver the beneficial property of *reciprocity*. Channel states estimated between two nodes hold the same value on both sides. Furthermore, an eavesdropper is not likely to obtain the same channel state. Therefore, the legitimate nodes establish an advantage, which they use to generate a secret key unknown to the eavesdropper. Usually, the legitimate users measure the current channel state by mutual *probing*. There are already quite a number of studies that show the principal feasibility of the approach. An early work [1] establishes an authentication by obtaining common information from the channel impulse response. This work was extended by subsequent studies with more emphasis on signal processing on the measured data [2], or advanced quantization strategies in order to increase reliability of the extracted key strings [3]. Further studies explored enhanced methods for removing statistical correlation between measured data, either block-based [4], or adaptively [5]. The work of [8] suggests a scheme for practical key agreement within the application of full-duplex near-field communication (NFC). Several studies establish the connection of theoretical secret-key rates from information theory to channel models of wireless environments, for instance [6]. Often, they assume that channel states are stationary and jointly Gaussian distributed.

However, most implementations for secret-key agreement from reciprocal wireless channels are realized by *half-duplex* (HD) nodes. Due to the HD constraint, channel probing is performed *consecutively*. This implies several drawbacks. Most significantly, an eavesdropper obtains two cleanly separated observations. Furthermore, in rapidly changing environments, the channel state might be already different after probing in one direction. This motivates a setup including *full-duplex* (FD) users. Recently, several research groups have demonstrated communication setups with FD capability, see [7], for instance. An implementation of FD nodes is challenging since the receiver suffers from *self-interference* (SI) inflicted by the own transmitter. As a consequence, appropriate techniques for SI *cancellation* need to be applied.

In secret-key agreement, FD channel probing is inherently providing additional protection against eavesdroppers, since the superposition of probing signals is leaking less information on the channel state than the subsequent probing in time-division duplex. To best of our knowledge, there is no comprehensive study on a practical implementation of secret-key agreement by FD-capable nodes.

In a recent work, we have investigated secret-key agreement in FD mode from a theoretical perspective [9]. In this work, we intend to verify and complement the theoretical model by practical measurements. We evaluate the performance of secret-key agreement by HD- and FD-capable communication nodes in a testbed. For this purpose, we implement FD-capable nodes with multi-stage SI cancellation. For the analysis, we propose a general system model that allows to quantify the correlation coefficients and mutual information based on the measurements obtained from channel probing. The potential capabilities of the eavesdropper need to be considered carefully, which in fact have often been disregarded [10]. Furthermore, it was pointed out [11] that the eavesdropper cannot be neglected even outside of the "half-the-wavelength" distance to the legitimate nodes, which was a popular assumption in many works before. We investigate the channel probing in more detail. In HD mode, there is always some delay between the probing of the two users. We analyze the impact of different delays. In FD mode, the users send pilots simultaneously, but

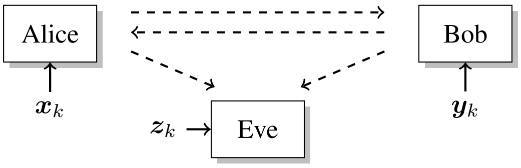

Fig. 1. Overview of the system model.

not necessarily synchronized. As already shown in the theoretical work [9], the superposition of probing signals downgrades the information that the eavesdropper can obtain. Therefore, the FD mode is always superior over the HD mode in terms of security. We study the effect of non-synchronized pilots on the eavesdropper in FD mode. However, since generally SI inflicts the quality of the channel estimation, there is a trade-off between enhanced security and possibly worse estimation quality.

The paper is organized as follows: Section II introduces the system model. In section III, the FD setup as well as the measurement protocol are described. Results are given in section IV, while the work is concluded in section V.

II. System model

The system model is depicted in Fig. 1. We consider three nodes Alice, Bob and Eve. The legitimate nodes Alice and Bob *probe* the channel in order to obtain estimates of the channel state. These measurements are frequently repeated by a fixed time interval. The users have different numbers of observations per probing. Generally, at each instant k, Alice gets x_k from the channel Bob-to-Alice, Bob obtains y_k from the channel Alice-to-Bob and Eve has real-valued vector observations $\boldsymbol{z}_k \in \mathbb{R}^2$ from the channels Alice-to-Eve and Bob-to-Eve, whereas x_k, y_k, $\boldsymbol{z}_k$ denote random processes.

Each element of $\boldsymbol{x}_k$ for a fixed k is correlated with all others (*per-vector correlation*). We have the desire to compress the statistical information in order to lower the dimension of $\boldsymbol{x}_k$, since entropy estimators show higher bias for large dimensions [14]. The tool of principal component analysis (PCA), is a popular method for extracting uncorrelated randomness [2]. Likewise, $\boldsymbol{x}_k$ is correlated to $\boldsymbol{x}_l$ at a different time l, which we denote as *process* or *temporal correlation*. In order to deal with this correlation, we model the time series as an linear auto-regressive (AR) vector process and perform linear vector prediction [12]. Bob and Eve perform the same steps with $\boldsymbol{y}_k$ and $\boldsymbol{z}_k$, respectively.

We assume independence of the uncorrelated data and drop the index k in the following. Subsequently, as the performance metric, we utilize mutual information of the channels estimates of Alice and Bob, Alice and Eve, Bob with $I(x, y)$, $I(x, \boldsymbol{z})$ and $I(y, \boldsymbol{z})$, respectively. Since the joint probability density function of $(x, y, \boldsymbol{z})$ is likely unknown in practice, mutual information has to be estimated from samples. For this purpose, we are going to utilize an entropy estimator based on the k-nearest neighbor estimator (NNE) from [14]. For the correlation coefficient, we use the estimator

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

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_k and y_k, respectively.

III. Measurements

In this section, we outline our implementation of the full-duplex setup and the measurement campaign. The testbed with nodes Alice, Bob and Eve is placed inside a laboratory. In order to obtain a reliable source of channel variations inside the room, we deploy a curtain of aluminum strips that rotates at ≈ 0.1 rotations per second in random directions.

A. Full-duplex setup

Since we want to compare secret-key generation of half-duplex and full-duplex nodes, we need to implement a FD-capable transceiver. The main challenge of FD communication is the self-interference (SI), which is very strong compared to any desired signal. Many possible solutions for self-interference cancellation (SIC) have been proposed already and most of them include three consecutive stages of SIC:

1) *Passive isolation* reduces the power leakage between transmitter and receiver at RF level,
2) *Active analog cancellation* invests some additional power at RF level in order to cancel out the SI,
3) *Digital cancellation* takes place after the Analog-to-Digital converter by means of digital signal processing.

Our implementation of SIC and the full-duplex node is depicted in Fig. 2. We use USRP (Universal Software Radio Peripheral) devices of Ettus Research company that allow for two-way communication. The main transmitter (Main TX) is supposed to transmit a signal to a distant node. For the passive isolation, we use a RF circulator. This circuit allows waveguiding only in clockwise direction, such that less power is leaked from Main TX into the receiver chain. Furthermore, we employ a second USRP. Its transmitter serves as an auxiliary signal generator (Aux TX) that is designed as an inverted copy of the SIC signal. The SI and Aux Tx signal cancel each other at the RF combiner. Subsequently, after sampling the received signal in Main RX, last steps of SIC can be done at a host PC in the digital domain. We utilize a FIR-filtered version of the transmitted signals in order to further reduce self-interference. The following table summarizes the SIC contribution of the three cancellation stages:

SIC stage	Amount
Passive isolation	25 dB
Active analog cancellation	25 - 30 dB
Digital cancellation	6 - 12 dB
Total	**60 - 65 dB**

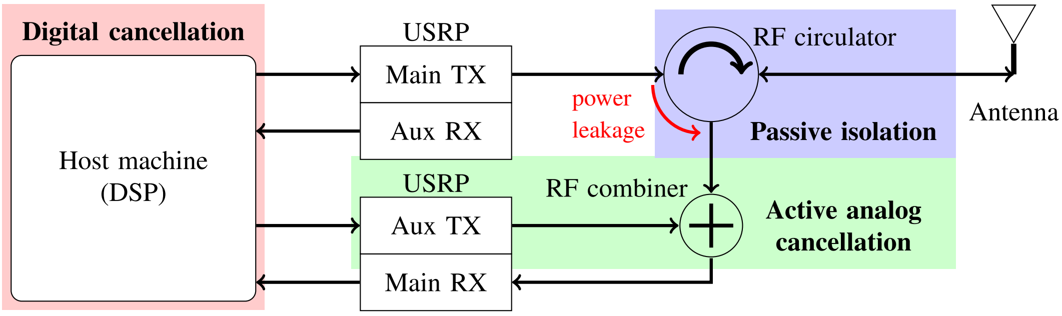

Fig. 2. Hardware setup of the full-duplex nodes.

TABLE I
PARAMETERS OF THE MEASUREMENT SETUP

Parameter	Variable	Value
Sampling rate	f_s	200 KSPS
Sampling interval	T_s	5 μsec
Center frequency	f_0	880 MHz
Samples per measurement	N	5000

In the literature, higher values are reported if nonlinearities and phase noise are considered in the SIC. However, since we are primarily interested in channel measurements for secret-key generation at rather small distance, this amount of SIC is sufficient.

B. Protocol

Alice and Bob exchange probing signals by OFDM frames based on the preamble of 802.11g PHY [15]. The oscillator frequencies of all devices are aligned, therefore, no frequency synchronization is required. From the viewpoint of security this is a worst-case assumption, since Eve benefits from the global synchronizations. The USRP devices offer the useful feature that transmitted signals can be precisely timed. Subsequently, we are able to create scenarios with either perfect or imperfect time synchronization for Alice and Bob, and consequently study its impact on Eve. We discuss the signal processing at Alice only, since it is essentially the same for Bob and Eve. At each time k, the channel state on every OFDM subcarrier is measured by channel estimation. After fine time synchronization and performing IDFT on the estimated channel transfer function, Alice gets the channel coefficients:

$$h_{k,n} = \alpha_{k,n} e^{j\phi_{k,n}} \qquad 0 \leq n \leq 63, \tag{2}$$

where $\alpha_{k,n}, \phi_{k,n} \in \mathbb{R}$. For subsequent analysis, we focus on the absolute value of the first tap $|h_{k,0}|$ only. We have similar observations at the other users. However, since the eavesdropper intercepts both probing signals, Eve has twice the observations available at each time k. Table I lists all the relevant parameters that characterize the protocol. In the following, we outline the signaling protocols for both HD and FD operation.

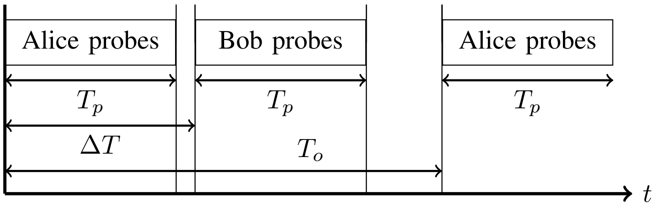

Fig. 3. Time-division duplex protocol in HD mode with probing duration T_p, ping-pong interval ΔT and observation interval T_o.

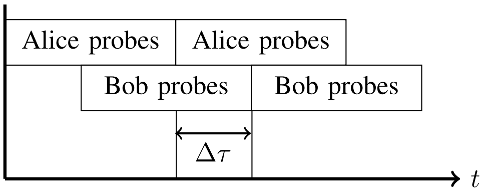

Fig. 4. Protocol in FD mode with relative delay $\Delta\tau$ between the probing signals.

1) HD mode

Since Alice and Bob have to share communication resources, we apply a time-division duplex protocol, which is depicted in Fig. 3 in simplified form. Alice and Bob broadcast probing signals with duration T_p. On the host machine, the transmission time of signals at both users is predetermined by timestamps. Therefore, we can control both the observation interval T_o between the updates of channel states and the time between the Alice's query and Bob's response, which we denote as "ping-pong" interval ΔT. It is desired to have ΔT as small as possible. If ΔT is in the order of the channel coherence time or larger, then the channel estimate of Alice and Bob are likely not to be correlated.

2) FD mode

In case of FD operation, generally the probing does not need to be synchronized. Signals are transmitted consecutively by Alice and Bob without any pause, as depicted in Fig. 4. However, the probing signals of Alice and Bob are superimposed with some fixed delay $\Delta\tau$ at the wireless medium. We control this delay by predetermining timestamps for the signals.

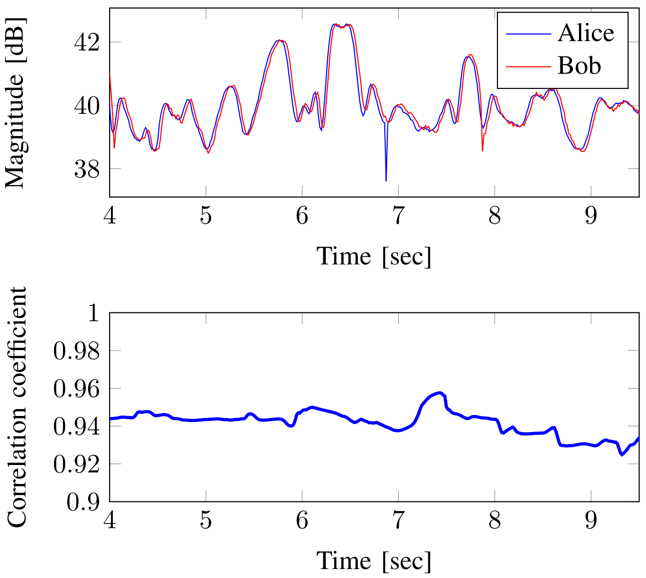

Fig. 5. Observations from channel estimations in FD mode.

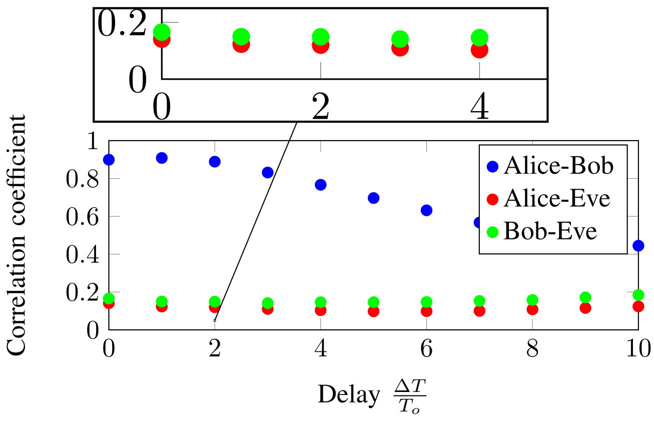

Fig. 6. Joint correlation coefficients of channels estimates in HD mode for different delays.

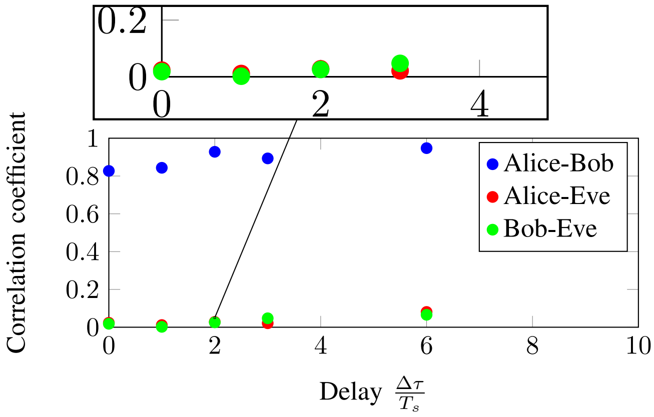

Fig. 7. Joint correlation coefficients of channels estimates in FD mode for different relative probing delays.

IV. Results

To demonstrate that the protocol operates successfully in FD mode, we begin with an example. Alice and Bob operate in FD mode as discussed in subsection III-B. Fig. 5 depicts the magnitude of the first tap of the channel impulse responses (upper figure) and the correlation coefficient (lower figure). The result demonstrates that Alice and Bob measure almost the same channel state. This is effectively shown by the correlation coefficient which remains at a high level around 0.94. It becomes apparent from the measurements that channel reciprocity is given in FD mode, thus Alice and Bob share a common secret. As a consequence, key generation is possible in FD mode.

A. Probing delay in HD mode

The result in HD mode is shown in Fig. 6. The correlation coefficients of channel taps are measured for different values of the delay ΔT, $T_p = 6.8$ msec and $T_o = 100$ msec, which denotes the time between the probing of Alice and Bob. Note that the result is obtained before the linear predictor is applied. In HD mode, the correlation of the observations of Alice and Bob drops if the “ping-pong” interval ΔT gets larger, since the channel is variant over time. We effectively have $\Delta T = 0$ in FD mode, because probing is done simultaneously. As expected, the correlation of the observations at Alice and Bob deteriorates if the delay increases. For smaller delays, there is some leakage of information to the eavesdropper, which can be seen in the magnified area of the figure.

B. Relative delay in FD mode

We study the capabilities of an eavesdropper in FD mode. We are averaging over 10 consecutive channel estimates each and perform downsampling by a factor of 6, which leads to an estimate on every 100 msec. Eve is intercepting the probing signals, but suffers from the superposition of the signals. The result of channel estimations is presented in Fig. 7 The correlation coefficients of channel taps are measured for different values of the relative delay $\Delta\tau$ between the probing of Alice and Bob. Apparently, the correlation coefficient of the channel estimates of Alice and Bob is large for all delays. Eve is only able to distinguish between the probing signals if they are transmitted with some relative delay $\Delta\tau$. Due to the superposition of the signals, even the synchronization of the probing signals is challenging for Eve. During our experiments, we synchronize all devices in time and frequency, and therefore, Eve always achieves perfect signal acquisition. Fig. 8 depicts the mutual information of all users for some $\Delta\tau$. The mutual information of the estimates of Alice and Bob changes for various delays. The reason for this might occur from the SI, since the superposition of probing signals might have an impact on the performance of SI cancellation. The leakage to the eavesdropper is small and barely changes for different values of $\Delta\tau$.

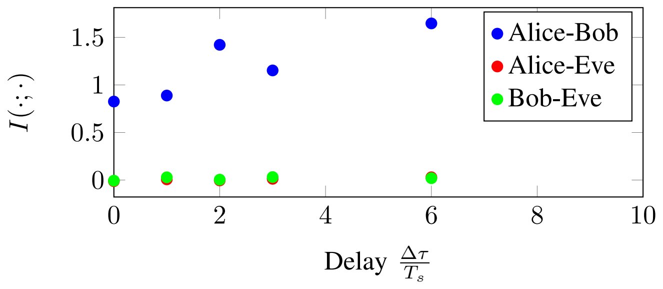

Fig. 8. Mutual information of channels estimates in FD mode for different relative probing delays.

V. Conclusion

In this work, we have investigated the performance of generating a common secret from reciprocal wireless channels by full-duplex (FD) probing. In order to verify the applicability of that approach, we have implemented a practical testbed with full-duplex capability. Due to the superposition of probing signals, an eavesdropper obtains few information on the main channel of Alice and Bob. Therefore, in FD communication systems, we obtain additional security of the secret-key material essentially "for free".

References

[1] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel," in *Proceedings of the 14th International Conference on Mobile Computing and Networking (MobiCom)*, 2008, pp. 128–139.

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

[3] J. Wallace, C. Chen, and M. Jensen, "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits," in *3rd European Conference on Antennas and Propagation (EuCAP)*, March 2009, pp. 1499–1503.

[4] C. Chen and M. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205–215, 2011.

[5] M. McGuire, "Channel estimation for secret key generation," in *Proc. Intl. Conf. on Adv. Inf. Netw. and App. (AINA)*, May 2014, pp. 490–496.

[6] G. Pasolini and D. Dardari, "Secret key generation in correlated multi-dimensional gaussian channels," in *Proc. Intl. Conf. on Communications (ICC)*, June 2014, pp. 2171–2177.

[7] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," in *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4. ACM, 2013, pp. 375–386.

[8] R. Jin, X. Du, Z. Deng, K. Zeng, and J. Xu, "Practical Secret Key Agreement for Full-Duplex Near Field Communications," *IEEE Trans. Mobile Comput.*, vol. PP, no. 99, pp. 1–1, 2015.

[9] H. Vogt and A. Sezgin, "Full-duplex vs. half-duplex secret-key generation," *arXiv:1506.08565*, 2015. [Online]. Available: http://arxiv.org/abs/1506.08565

[10] W. Trappe, "The Challenges Facing Physical Layer Security," *IEEE Comm. Mag.*, vol. 53, no. 6, pp. 16–20, 2015.

[11] A. J. Pierrot, R. A. Chou, and M. R. Bloch, "Practical limitations of secret-key generation in narrowband wireless environments," *CoRR*, vol. abs/1312.3304, 2013. [Online]. Available: http://arxiv.org/abs/1312.3304

[12] P. Vaidyanathan, *The Theory of Linear Prediction*. Morgan & Claypool, 2007. [Online]. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6813346

[13] M. R. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[14] A. Kraskov, H. Stögbauer, and P. Grassberger, "Estimating mutual information," *Physical Review E*, vol. 69, no. 6, p. 066138, 2004.

[15] "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," *IEEE Std. 802.11g*, vol. Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, 2003.