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 theoretically achievable secret-key rates based on the measured data and compare the performance to conventional half-duplex setups. 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. 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]. 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. We are aware of a single work that considers a practical FD setup for key agreement [8], but it is limited to near-field communication only.

In a recent work, we have investigated secret-key agreement in FD mode from a theoretical perspective [9]. In this work, we compare the performance of secret-key agreement by HD- and FD-capable communication nodes in a practical 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 theoretically achievable secret-key rate 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]. Consequently, we insert other nodes that represent a passive, but *multiple*-terminal eavesdropper in the scene. 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 not necessarily synchronized. We study the effect of non-synchronized pilots on the eavesdropper.

II. System model

The system model is depicted in Fig. 2. We consider

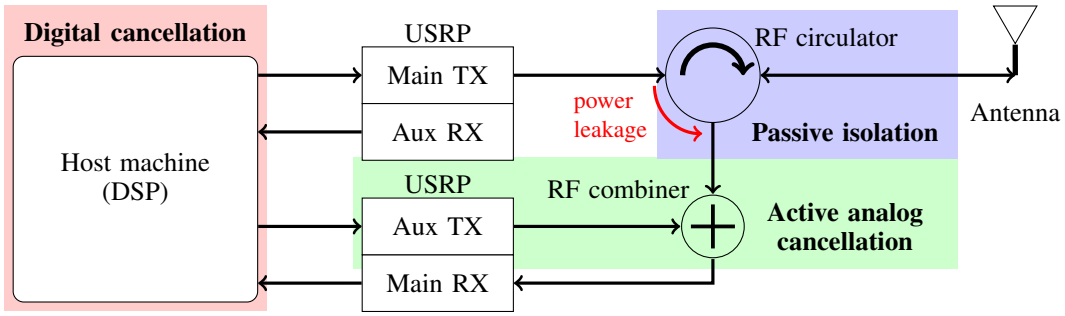

Fig. 1. Hardware setup of the full-duplex nodes.

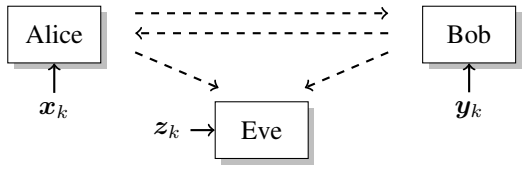

Fig. 2. Overview of the system model.

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. Complex-valued channel states account for two real-valued measurements. Eve holds multiple nodes and therefore can combine all observations. Generally, at each instant k, Alice gets the real-valued vector observations $\boldsymbol{x}_k$, Bob obtains $\boldsymbol{y}_k$ and Eve has $\boldsymbol{z}_k$, whereas $\boldsymbol{x}_k$, $\boldsymbol{y}_k$, $\boldsymbol{z}_k$ denote random vector 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 performs the same steps with $\boldsymbol{y}_k$.

We assume independence of the uncorrelated data. Subsequently, we utilize a lower bound on secret-key capacity [13]. Since the joint probability density function 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].

III. Measurements

In this section, we outline our implementation of the full-duplex setup and the measurement campaign.

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. 1. 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**

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 USRP

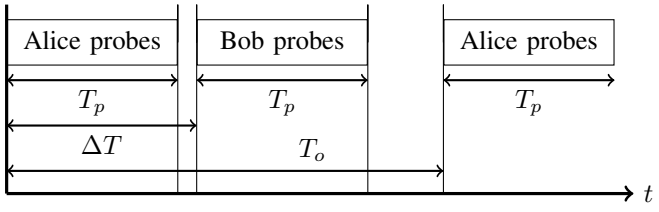

Fig. 3. Time-division duplex protocol in HD mode with probing duration T_p, ping-pong interval ΔT and observation interval T_o.

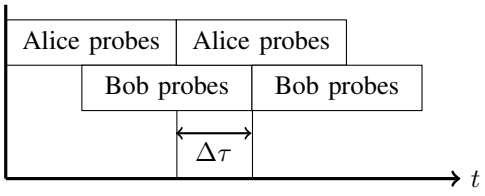

Fig. 4. Protocol in FD mode with relative delay $\Delta\tau$ between the probing signals.

devices offer the useful feature that transmitted signals can be precisely timed. Subsequently, we are able to create scenarios with either perfect or imperfect synchronization for Alice and Bob, and consequently study its impact on Eve. In the following, we outline the signaling protocols for both HD and FD operation.

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.

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.

IV. Preliminary Results

We present some preliminary results here, more results are shown in the final paper. 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

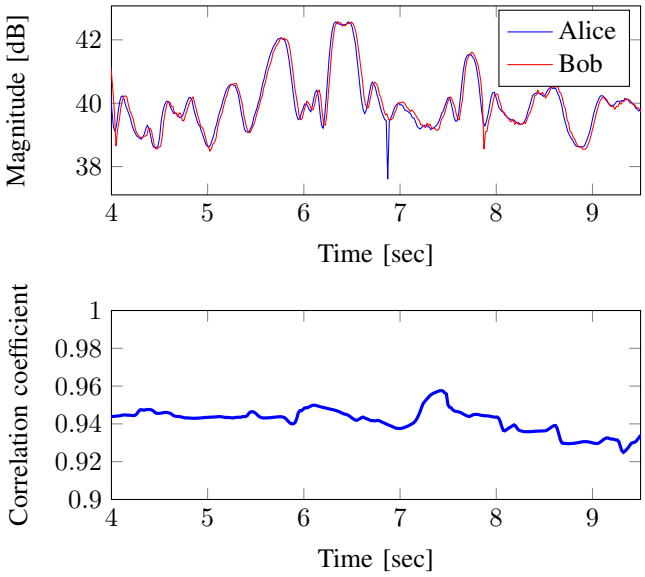

Fig. 5. Observations from channel estimations in FD mode.

in FD mode. Subsequent studies will build on this fact and investigate the following:

- 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. On the downside, the estimations in FD mode suffer from residual self-interference. We find the interval ΔT for which HD and FD mode have similar performance in terms of key rates.
- We study the (potentially worse) capabilities of an eavesdropper in FD mode. Eve is intercepting the probing signals but suffers from the superposition of the signals. Still, Eve is able to distinguish between the probing signals if they are transmitted with some relative delay $\Delta\tau$. We are going to identify delays which are most unfavorable for an eavesdropper.
- We investigate whether observations on multiple terminals strengthen the eavesdropper significantly.

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.