Wireline Physical-Layer Key Generation

Werner Henkel, Oana Graur, and Uwe Pagel

Transmission Systems Group (TrSyS), Jacobs University Bremen, e-mail: werner.henkel@ieee.org

Abstract

Physical layer security is typically linked to TDD wireless applications, where roughly a reciprocity of the channel can be assumed. This creates the required common randomness and protection against eavesdropping. In here, we show that a wireline connection, be it power line or twisted pair, offers the necessary symmetry and protection against eavesdropping, as well. Randomization is possible, but is not yet discussed in detail.

Index Terms

Physical-layer security, key generation, power line, PLC, DSL, Ethernet, twisted pair, TP, UTP, IoT

I. Introduction

Physical-layer security is typically seen in conjunction with TDD wireless links together with the assumption that the channel will not change significantly between the time slots for both directions. There is a vast literature, where we can only list a few references. A standard reference discussing different kinds of physical-layer security, be it Wyner's wiretap channel or key generation with it secrecy and secret key capacities, respectively, is certainly the book by Bloch and Barros [1]. Otherwise, Trappe and Wade give some overview posing major questions in [2]. Randomization using RECAP antennas was discussed in [3]. Our own publications were, so far, concentrating on quantization and key reconciliation [4]–[7]. Having looked into wireless systems to provide common randomness, especially with TDD, we asked ourselves, if cable loops would not provide this common randomness as well. There, the transfer and far-end crosstalk (FEXT) functions are, of course, obvious candidates. However, one has to additionally ensure that an eavesdropper has, at least, worse possibilities to obtain a similar key.

II. Reciprocity for key generation between power outlets and on Ethernet cables

We describe some initial investigations, using power line cables and twisted pairs isolated or inside the network. It is obvious that the transfer function of a homogeneous wire pair is symmetric, which we will see still carries over to inside a network. This is not completely obvious, since two-port matrix products are, of course, not commutative. The Far-End crosstalk (FEXT) function would also be an alternative, which is known to be of a more stochastic nature over frequency. The FEXT function is very symmetric on an isolated cable, as well, not so in an actual network, due to the network topology with bridge taps to appliances or even with open ends (not connected power outlets). In here, we show some initial measurements using a specially designed interface circuit holding both transmitting and receiving sides. Due to space limitations, we can only show the transfer function after a normalization, smoothing, and offset elimination step up to 30 MHz in Fig. 1. Higher frequencies do not reliably provide nice reciprocity properties. All transfer functions up to 30 MHz, be it on L-N or N-PE pairs yield nice symmetry properties that allow, e.g., to detect the location of maxima, which one can easily use to map the positions to binary bit pattern of a to be generated key sequence. L-N and N-PE measurements may show similar or completely different frequency responses, however, always almost perfectly reciprocal. We added some exemplary quantization regions using different grey levels into the plot. For key reconciliation purposes, one can introduce guard intervals, such as shown for another transfer function measurement in Fig. 2. A peak would be discarded when ending up inside the (white) guard space. Other reconciliation procedures might, e.g., additionally use Slepian-Wolf coding [4].

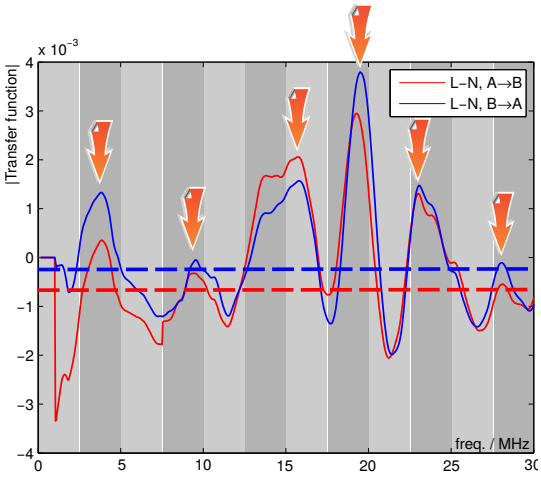

Fig. 1: L-N transfer functions and quantization (calibrated and smoothed)

Quantization tables can, e.g., be established according to the number of peaks e offering max $\binom{N}{e}$ entries with corresponding bit patterns. As indicated in Fig. 1, one may use separate thresholds for both directions to ensure that the numbers of peaks are identical. Hence, there needs to be a protocol in place to 'agree' on the number of peaks, i.e., the use of the same bit pattern table.

The phase properties, shown as phase differences between frequency samples (≈group delay) in Fig. 3 shows also reciprocity properties to some extent, but not as prominent to be suited for key generation purposes. FEXT functions, e.g., from the L-N to the N-PE loop, were typically not showing a suitable reciprocity as visible in Fig. 4.

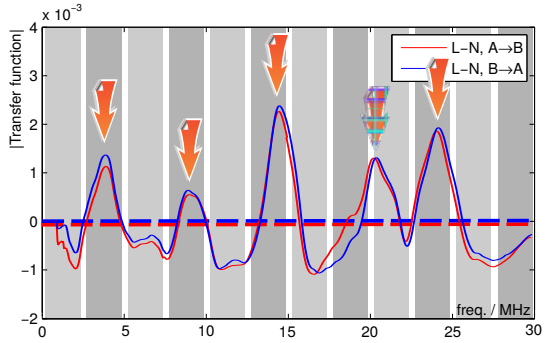

Fig. 2: L-N transfer functions, quantization with guard intervals (cal. and smoothed)

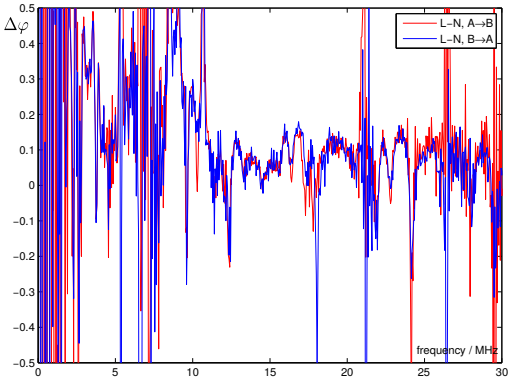

Fig. 3: L-N loop group delay functions

Additional to showing the desired reciprocity, the transfer function differs significantly to different power outlets, where possibly eavesdropping devices could be located.

However, not only reciprocity is required, but also a certain randomness. Without further measures, only switched appliances would create some randomness. A further randomization is possible with variable bridge taps or variable loads. This is not yet discussed in here.

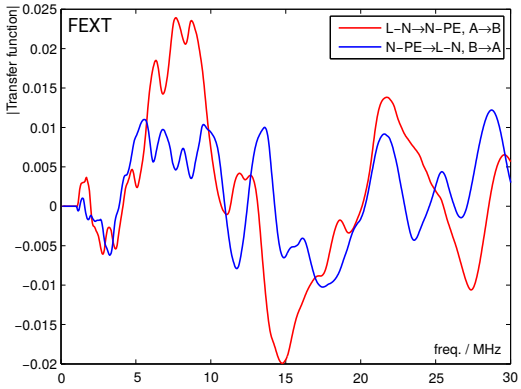

Fig. 4: FEXT between L-N and N-PE loops (cal. and smoothed)

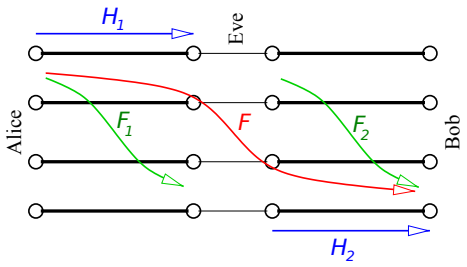

Fig. 5: Arrangement and measured functions of loop segments

Looking into point-to-point connections, the FEXT function still provides sufficient reciprocity, too. For a more or less homogeneous cable, we could require that the overall FEXT function cannot easily be computed from partial knowledge of an eavesdropper.

For convenience and to illustrate the principle, we show FEXT functions measured at a 25 m / 50 m twisted pair arrangement (CAT 5) shown in Fig. 6. In red, two-sided FEXT-measurements are shown (hardly distinguishable), while the blue $\hat{F}$ is a closest estimate of a wiretapping eavesdropper. This closest estimate of the overall FEXT function results from

$$F \approx \hat{F} = F_1 \cdot H_2 + H_1 \cdot F_2 \ , \qquad (1)$$

making use of the segment transfer functions H_1 and H_2 and the segment FEXT functions F_1 and F_2 (see Fig. 5) that the eavesdropper might have access to.

It is clearly visible that the estimate shows the rough trend, as well, but definitely not the same fluctuations and notches, thereby allowing secure key generation. FEXT functions are stronger in power cables, since they are not symmetric and not twisted as their telephone and Ethernet counterparts.

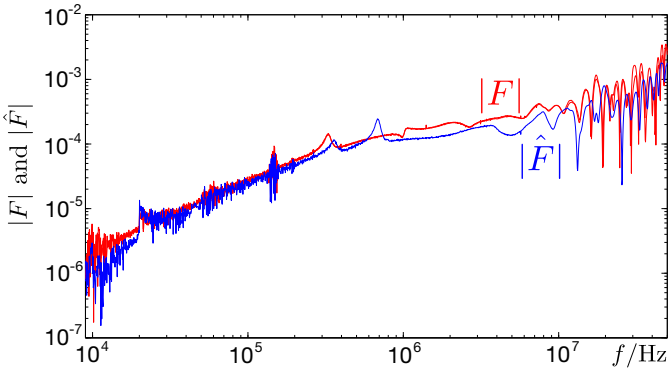

Fig. 6: FEXT function and an eavesdropper's estimate (CAT 5)

Randomness in the case of FEXT can be realized by randomly modifying coupling/grounding of/to other loops in the neighborhood, thereby contributing to FEXT.

III. Conclusions and further research

We have given an indication that physical-layer methods can also be applied to wireline connections, be it power line or twisted pairs. In power line communication, the transfer function itself appears suitable for this task, whereas FEXT with the inherent randomness along frequency is preferred for a point-to-point connection (be it power line or Ethernet). The transfer function in a homogeneous cable is not usable, since it can easily be calculated by an eavesdropper due to its deterministic nature.

Power lines seems to be the more interesting channel for physical-layer key generation, due to upcoming IoT (Internet of Things) applications. When home and other appliances are communicating over the power lines, a certain amount of secrecy should be guaranteed and physical layer security, just using the properties of the power line connection, appear as the appropriate solution, even if the mutual information between the legitimate and eavesdropper channels may not perfectly be zero. However, privacy amplification can solve secrecy deficits [1]. Since power line communication uses multicarrier modulation (DMT) the complex transfer function at every carrier location is determined at the receiver and the basis for key generation is hence readily available.

References

[1] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.
[2] W. Trappe, "The Challenges Facing Physical Layer Security," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 16–20, 2015.
[3] R. Mehmood and J. W. Wallace, "Experimental Assessment of Secret Key Generation using Parasitic Reconfigurable Aperture Antennas," *Proceedings of 6th European Conference on Antennas and Propagation, EuCAP 2012*, no. 1, pp. 1151–1155, 2012.
[4] N. Islam, O. Graur, A. Filip, and W. Henkel, "LDPC Code Design Aspects for Physical-Layer Key Reconciliation," IEEE International Global Communications Conference, 2015.
[5] O. Graur, N. Islam, A. Filip, and W. Henkel, "Quantization Aspects in LDPC Key Reconciliation for Physical Layer Security," *10th International ITG Conference on Systems, Communications and Coding*, pp. 1–6, 2015.
[6] O. Graur, N. Islam, A. Filip, and W. Henkel, "Quantization and LLR Computation for Physical Layer Security," in *International Zurich Seminar on Communications*, 2016.
[7] J. Wallace, W. Henkel, O. Graur, N. Islam, R. Mehmood, R. Sharma, and A. Filip, "Physical-Layer Key Generation and Reconciliation," in *Communications in Interference Limited Networks*, Springer, 2016.