Electronic Communications of the EASST
Volume 080 (2021)

Conference on Networked Systems 2021
(NetSys 2021)

Ray-tracing based Inference Attacks on Physical Layer Security

Paul Walther, Markus Richter and Thorsten Strufe

4 pages

ECEASST Home Page: http://www.easst.org/eceasst/ ISSN 1863-2122

Ray-tracing based Inference Attacks on Physical Layer Security

Paul Walther[1], **Markus Richter**[1] **and Thorsten Strufe**[2]

[1] Chair for Privacy and Security, TU Dresden
[2] Karlsruhe Institute of Technology (KIT) and Centre for Tactile Internet, TU Dresden (CeTI)

Abstract: In wireless network security, physical layer security provides a viable alternative to classical cryptography, which deliver high security guarantees with minimal energy expenditure. Nevertheless, these cryptograhpic primitives are based on assumptions about physical conditions which in practice may not be fulfilled.

In this work we present a ray-tracing based attack, which challenges the basic assumption of uncorrelated channel properties for eavesdroppers. We realize this attack and evaluate it with real world measurement, and thereby show that such attacks can predict channel properties better than previous attacks and are also more generally applicable.

Keywords: Wireless Network Security, Physical Layer Security, Attack

1 Introduction

Physical Layer Security (PhySec) promises to provide an alternative to classical encryption. Information theoretic proofs demonstrate its high security guarantees [BB11]. Additionally, it has low computational complexity and minimal energy consumption. This combination makes it very enticing for resource constrained devices, e.g. in sensor networks, IoT or the Tactile Internet. PhySec exploits the properties of the physical medium to achieve security goals and it provides primitives for encryption, authentication and key derivation. Despite the security proofs, the security is based on assumptions about the leveraged physical properties, which we deem questionable in realistic settings.

PhySec is well suited for implementation in the field of wireless network security, as there is a multitude of physical properties that can be exploited for this purpose. Authentication and key generation use the channel coefficients of the shared channel between the legitimate terminals to derive unique identifiers, or symmetrical keys respectively. These properties of the wireless channel are completely described by the *Channel Impulse Response* (CIR) [Gol05]. The underlying security assumption in this context is derived from the so called *Uniform Scattering* model developed by Jakes [Jak95]. This assumption states, that an adversary residing more than half of a wavelength away from the legitimate terminals can only measure channel characteristics uncorrelated to those of the legitimate shared channel. If this assumption is not fulfilled, the attacker can observe channel properties with high correlation to the legitimate ones. This would mean that despite the proven security of the subsequent processing, the security primitives themselves must be considered compromised. Here we want to collect evidence to determine whether this assumption is justified in the PhySec context or not.

In continuation of this rationale, practical attacks have already been presented, which aim at directly predicting the CIR of the legitimate channel [WKS20, B^+12]. Such attacks have the following advantage: Due to noise and interference, differences between observations also occur between the channel characteristics of the legitimate partners. The further processing of the CIRs for PhySec primitives takes this into account and removes such differences [BB11]. This gives the attacker the advantage that no perfect prediction is necessary to compromise the corresponding security primitive.

Although the presented approaches demonstrate the basic feasibility of such attacks, they come with the disadvantage that they are not generally applicable yet. More precisely, they either achieve very little agreement between the legitimate and the predicted properties (even less than simple eavesdropping) or they are applicable to a very specifically given setting only.

In this paper we present an alternative prediction attack based on ray-tracing concepts. This has the advantage that predictions about channel properties can be realized based solely on geometry and terminal position. Thus, in contrast to the current state of the art, this attack is both generally applicable and completely independent of any kind of optimization. We will show that high correlation between the predictions and the actual channel properties can still be achieved.

We implement the presented attack and evaluate it with real world measurements. The results are then compared to current state of the art attacks. Finally, to demonstrate the effects of such attacks, we show that in the context of key derivation a significantly lower hamming distance is achieved than for an eavesdropping adversary.

2 Ray-tracing based Inference Attacks

The **core approach** of our attack is to directly predict the channel properties of the reciprocal channel shared by the legitimate partners. Given an accurate enough prediction, the adversary can perform the same processing as Alice and Bob and thereby achieve the same results, e.g. the same key material. The rationale for a ray-tracing based attack on CIRs is twofold:

First, ray-tracing based simulations are very well suited for simulating wave propagation for high frequency electromagnetic waves [YI15]. In such settings, the power received at the target terminal can be simulated as the superposition of all relevant rays. Hence, this method is suitable to simulate the amplitude of the resulting CIR with high accuracy [YI15].

Second, the ray-tracing calculation can be executed completely offline, without specific knowledge of the actual transmission. The only parameters required for the simulation are room geometry, terminal positions and wireless frequencies. All of these are accessible to attackers, since they can either be observed directly or are system parameters.

Together, these two reasons make the ray-tracing method an easy to implement but nevertheless promising method for the prediction of CIRs.

Within this system we assume the following **attacker model**: the adversary is a passive eavesdropper, equipped with standard COTS hardware. No setup steps for this attack need to be conducted. To carry out this attack, an adversary only needs to know the room geometry and the positions of the legitimate terminals, both of which can be easily obtained, e.g. by visual inspection.

This attack model assumes a much weaker attacker than related works [WKS20, B$^+$12], as it does not require a preparatory phase in which the attacker collects specific measurements in the attacked room. Additionally, no optimization with respect to these collected samples is required.

To **execute** such an attack, an adversary would proceed as follows: In a first step a representation of the current environment would be created — considering the typical use case of indoor wireless communication, this can be realized with negligible effort since most indoor rooms have cuboid shapes, which are easily modelled. During the actual attack, the attacker evaluates the ray-tracing model given the environment and the terminal position of the legitimate partners. These positions can be obtained visually at the point in time, at which the reciprocal measurement is conducted (which can be overheard by the adversary). The result of the ray-tracing simulation is then processed analogous to the actual key derivation. No actual observation of the legitimate partners exchange is required.

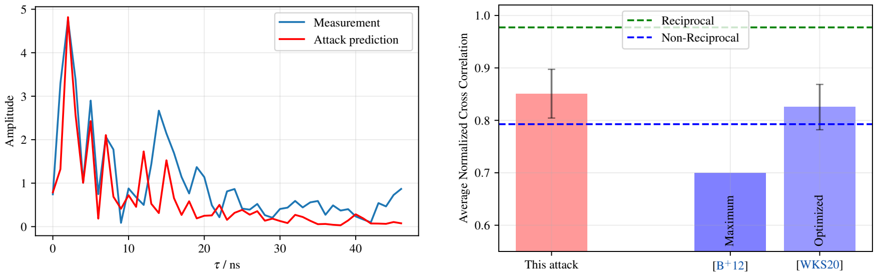
3 Realization and Evaluation

The **metric** used to evaluate the accuracy of our predictions is the normalized cross-correlation as defined in [Mit16]:

$$cc(g,h) = \max_k \frac{r_{gh}(k)}{\sqrt{E_g E_h}} = \max_k \frac{\sum_{i=-\infty}^{\infty} g[i]h[i-k]}{\sqrt{\sum_{i=0}^{n_g-1} g[i]^2 \sum_{i=0}^{n_h-1} h[i]^2}}.$$

This calculates the cross correlation cc between the two signals g and h as a metric of the similarity. Here, r_{gh} is the non-normalized cross-correlation and E_g and E_h is the energy of the respective signal. In the concrete case g and h are the actual legitimate CIR and the respective prediction from the ray-tracing attack. Related work [WKS20, B$^+$12] use this metric as well, which facilitates a direct comparison.

The **dataset** used for evaluation is the same as presented in [WKS20]: the samples are CIRs of ultra-wideband transmissions, realized with a center frequency of 4GHz and a bandwidth of 500MHz. We measured 17 different setups with 1000 CIRs each in a typical indoor environment.



(a) Prediction example

(b) Comparison of different attacks

Figure 1: Evaluation results of the proposed ray-tracing attack.

Our implementation of the ray-tracing based attack using PyLayers [ALU13] achieved the following **results**.

To demonstrate the general prediction performance, Fig. 1a shows a direct comparison of a measured CIR with the corresponding prediction from the ray-tracing attack. The core characteristics of the CIR were accurately predicted by the attack.

To further assess the effectiveness and to compare it against the state of the art, the average cross correlation achieved with this attack is present in Fig. 1b. The dotted lines represent the average correlation of the legitimate, reciprocal CIRs as well as the eavesdropped ones, i.e. the non-reciprocal CIRs. The cross correlation of the proposed attack is shown as red bar on the left; the relevant related work are shown as blue bars on the right. The proposed attacks achieved a cross correlation of 0.851. This is higher than the maximum of 0.7 for [B^+12] and higher than the average 0.825 for [WKS20]. This means that our attack can more accurately predict the legitimate channel characteristics than the compared attacks. For [WKS20] we compare our results against their general optimization as we want a generally applicable attack.

The results show that the ray-tracing attack presented here achieves a better average cross correlation than comparable inference attacks. Additionally, these results were achieved without any training or optimization. Hence, this attack is more generally applicable and still outperforms the compared attacks.

4 Summary

In this work we investigated whether an adversary can directly predict channel properties used in Physical Layer Security through ray-tracing based simulations. We realized such an attack and evaluated it on real world measurements. The results showed how this kind of attacks can achieve better correlated predictions than related works, while being more generally applicable and without the need for any optimization.

Bibliography

[ALU13] N. Amiot, M. Laaraiedh, B. Uguen. PyLayers: An open source dynamic simulator for indoor propagation and localization. In *IEEE ICC*. 2013.

[B^+12] S. Ben Hamida et al. On the Security of UWB Secret Key Generation Methods against Deterministic Channel Prediction Attacks. In *IEEE VTC*. 2012.

[BB11] M. Bloch, J. Barros. *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[Gol05] A. Goldsmith. *Wireless Communications*. Cambridge university press, 2005.

[Jak95] W. C. Jakes (ed.). *Microwave Mobile Communications*. An IEEE Press Classic Reissue. IEEE Press [u.a.], New York, NY, nachdr. edition, 1995.

[Mit16] S. Mitra. *Signals and Systems*. Oxford Series in Electrical and Computer Engineering. Oxford University Press, 2016.

[WKS20] P. Walther, R. Knauer, T. Strufe. *Passive Angriffe auf kanalbasierten Schlüsselaustausch*. Gesellschaft für Informatik e.V., Bonn, 2020.

[YI15] Z. Yun, M. F. Iskander. Ray tracing for radio propagation modeling: Principles and applications. *IEEE Access* 3, 2015.