# Poster: AnaMPhy: Anonymity Assisted Secret Key Refreshment

Jay Prakash
SUTD, Singapore

Rajesh Pachigolla
Synopsys India Pvt Ltd., India

Aman Goyal
UCSD, USA

Parthajit Mohapatra
IIT Tirupati, India

Tony Q.S. Quek
SUTD, Singapore

## ABSTRACT

This work is motivated by the fact that the secret key generation and refreshment of the key at the physical layer, based on randomness from reciprocity in the wireless channel, is challenged by little variations in the channel, particularly in an indoor environment. We propose a new technique, AnaMPhy, which uses multi-fold anonymity to refresh key at a high rate at two participating transceivers. The key generation and agreement in AnaMPhy is functional in challenging environments with very low or no variations in wireless channels. The idea is to hide the identity of the transmitter and the receiver, using medium access control (MAC) and physical layer strategies (randomization in oscillator drift ), and use pulse amplitude modulation (PAM) symbols to confuse and adversary. The secret key is the function of the message's source, chosen symbols and the channel's state. In doing so, confusion at the adversary increases manifold and Alice and Bob are able to refresh their secrets whenever needed. The proposed method is also implemented on software-defined radio (SDR). We argue that key refreshment using low complexity secret refreshment of AnaMPhy would be critical for decentralized systems in IoT and cyber physical systems (CPS) networks.

## CCS CONCEPTS

• **Security and privacy → Mobile and wireless security**;

**ACM Reference Format:**
Jay Prakash, Rajesh Pachigolla, Aman Goyal, Parthajit Mohapatra, and Tony Q.S. Quek. 2020. Poster: AnaMPhy: Anonymity Assisted Secret Key Refreshment. In *13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '20), July 8–10, 2020, Linz (Virtual Event), Austria.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3395351.3401704

## 1 INTRODUCTION

Physical-Layer-Security (PLS), generation of shared secret from randomness in wireless channel, has gained significant attention both from information theory research community and security and system design researchers in the last decade [4]. At the core, PLS is motivated by the principle of reciprocity, similar channel at uplink and downlink transceivers when measured within the coherence time. In practice, secret key generation is limited by environment and motion of scatterers since they affect the coherence time [3]. When IoT networks and CPS would be deployed in environments where the wireless channel is static, coherence time is large, such as in indoor environments, it would be a challenging task to generate and refresh secret keys at necessary rates. One of the common assumptions involved in physical layer secrecy is that eavesdropper knows the identity of users. However, de-anonymzing the source of packets is a non-trivial problem and anonymity of users can act as a source of randomness. In this paper, we aim to answer the two research questions: **RQ 1:** How to prevent the attack on the physical layer from breaking the anonymity of transceivers? **RQ 2:** How can the anonymity of users be used as a resource for physical layer secret key generation and refreshment?

In this paper, we focus on mitigating attacks on the anonymity of transceivers which is based on the drift of the local oscillator and propose how we can exploit the anonymity for secret key generation at the physical layer. The main contributions of the work are: (a) a novel cross-layer anonymization scheme is proposed based on a random drift in the local oscillator of transceivers and (b) a randomized version of Pulse Amplitude Modulation (PAM) is proposed to facilitate secret key generation under transceivers' anonymity. The proposed scheme is formulated as a multiple hypothesis testing problem whose performance is to be analyzed under Bayesian framework.

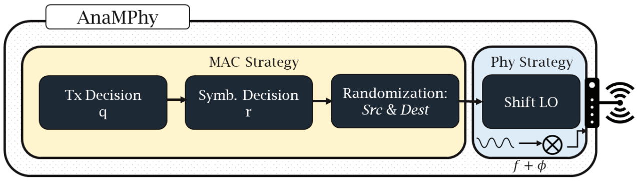

**Figure 1: Protocol strategy across different layers (Alice)**

### 1.1 AnaMPhy Transmission Strategies

As shown in Fig. 1, the protocol has defined strategies at both medium access control (MAC) and physical layer to facilitates environment independent generation of secret keys. **MAC Strategy:** As part of medium access, each coherence time is divided in to M slots, $T_{C1}$ : $T_{C5}$ in Fig. 2. For each of the M slots, Alice (Bob) makes decision of whether to transmit or to remain silent. Alice and Bob get a slot for transmission with probability $p$ and $1-p$, respectively. Further, given a slot Alice (or Bob) makes a decision to transmit with probability $q$ (or $s$) and decides not to transmit with probability $1-q$ (or $1-s$). If Alice (or Bob) decides to transmit, it sends symbols $A_1$ (or $A_2$) and $-A_1$ (or $-A_2$) with probabilities $r$ (or $t$) and $1-r$ (or $1-t$), respectively. It is also assumed that $A_2 > A_1$ without loss of generality. Given a slot, the choice of transmitting or not transmitting is independently and randomly decided by the users binding to the prior probabilities as mentioned in next subsections. Once the symbol is finalized, the transmitter randomizes packet source (`src`) and destination (`Des`) fields.

*WiSec '20, July 8–10, 2020, Linz (Virtual Event), Austria*
© 2020 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-8006-5/20/07.
https://doi.org/10.1145/3395351.3401704

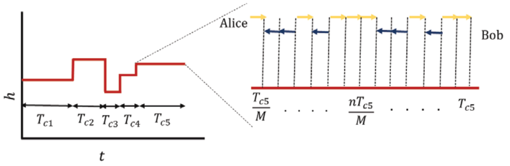

**Figure 2: Medium access scheme during stable channel**

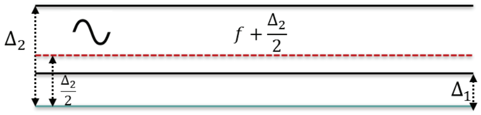

**Figure 3: Oscillator drift randomization**

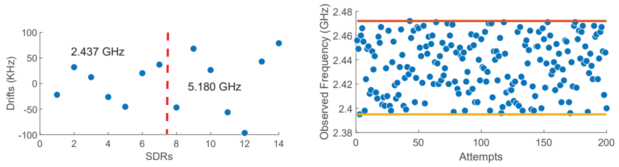

**Figure 4: Individual drifts at Channel 7 and 36**

**PHY Strategy: Challenge to Wireless Anonymity**: Wireless anonymity can be referred to as a state of confusion at the eavesdropper regarding the source of packet. Two important challenges for physical layer anonymity are a) RF Fingerprinting (received signal strength (RSS) or wireless channel impulse response) and b) properties of local oscillator (LO). Eve, adversary, can differentiate between source and sink using the uniqueness in frequency offset in LO of a RF chain [2]. In order to maintain LO base anonymity at physical layer, we propose a new frequency drift randomization technique so that Eve cannot learn uniqueness of the LO drift in a given time frame. Suppose $f$ is the desired central frequency of the frequency oscillator. Alice and Bob have drifts of $\Delta_1$ and $\Delta_2$ respectively. In order to anonymize packet source, we introduce artificial random shifts at both Alice and Bob. As shown in Fig (3), the goal is to insure that the final oscillator frequency is chosen from a source with mean of $f + \Delta_2/2$ and variance of $\Delta_2/2$ and hence the ambiguity is maintained. In order to maintain the position of final drift, as observed by Eve, within above mentioned range, Alice will choose an artificial frequency drift from Gaussian distribution with mean $\Delta_2/2 - \Delta_1$ and variance $\Delta_2/2$. Bob will choose drift with both mean and variance of $\Delta_2/2$ and. This would ensure that their frequency, as observed by Eve is same and random shifts will confuse her regarding the source (sink) of the packets. We note that Alice can be made aware of the drift at Bob using state-of-art key generation method at physical layer [4]. In practice there exists frequency drift, expressed in tolerance as parts per million (ppm) due to imperfections in oscillator of a typical transceiver. A tolerance of $f_{tol}$ ppm means that the oscillator may deviate from the desired frequency of $f$ GHz by up to $f \cdot f_{tol}$ kHz in either direction, i.e., $f \pm f \cdot f_{tol}$ kHz. We tested across 7 NI-USRPs i.e., 21 Alice-Bob pairs. The observed drifts are plotted in Fig. 4. As can be seen, the observed oscillator drifts ranged between -42 KHz to 35 KHz for 7 USRPs at channel 6, 2.437 GHz, and is more pronounced as we shift to higher frequency band i.e., channel 36. A random frequency shift in accordance with the proposed methodology was introduced using digital frequency shifting functionality provided by LabView Communication Design Suite [1].

## 1.2 Detector Design: Bayesian Framework

For error analysis, in the detection of symbols and its source, the proposed scheme can be viewed as a randomized version of the pulse amplitude modulation (PAM) where Alice or Bob can choose to transmit at $A_1$ ($A_2$), $-A_1$ ($-A_2$) or decide to remain silent based on the MAC transmission strategy. It is assumed that the prior probabilities of transmitting or remaining silent are known at all the participating nodes. The detection of symbols at the receiving nodes can be formulated as a hypothesis testing problem under the Bayesian framework. We exploit the fact that Eve has higher uncertainty about the received symbols and its source. The hypothesis testing problem at various nodes are discussed ahead. Alice needs to distinguish on which level Bob has transmitted, i.e., $\pm A_2$ or decided to remain silent. The possible hypotheses at Alice are $H_0^A : y_{a,i} = z_i$, $H_1^A : y_{a,i} = A_2 + z_i$, and $H_2^A : y_{a,i} = -A_2 + z_i$, where i= 1, 2, …, N and $z_i \sim \mathcal{N}(0, \sigma^2)$. The PDF under hypothesis $H_i^a$ is distributed as $\mathcal{N}(A_i, \sigma^2)$, where $A_i = 0, A_2$, or $-A_2$ for $i = 0, 1,$ or 2, respectively. In a similar manner, one can define the different hypothesis and their corresponding PDF for Bob. Using Bayes decision rule, the multiple hypothesis testing problem at Alice reduces to the following

$$\frac{1}{N}\sum_{i=1}^{N} y_i^a \underset{H_0/H_2}{\overset{H_1/H_2}{\gtrless}} th_{b1}, \frac{1}{N}\sum_{i=1}^{N} y_i^a \underset{H_0/H_1}{\overset{H_2/H_1}{\lessgtr}} th_{b2},$$

$$\text{and } \frac{1}{N}\sum_{i=1}^{N} y_i^a \underset{H_2/H_0}{\overset{H_1/H_0}{\gtrless}} th_{b3},$$

where $th_{b1} \triangleq \frac{\sigma^2}{NA_2}\ln\frac{p_{0a}}{p_{1a}} + \frac{A_2}{2}$, $th_{b2} \triangleq \frac{\sigma^2}{NA_2}\ln\frac{p_{2a}}{p_{0a}} - \frac{A_2}{2}$ and $th_{b3} \triangleq \frac{\sigma^2}{2NA_2}\ln\frac{p_{2a}}{p_{1a}}$. Note that $w \underset{H_0/H_2}{\overset{H_1/H_2}{\gtrless}} u$ means, if $w \geq u$ then either of $H_1$ or $H_2$ is true; otherwise, either of $H_0$ or $H_2$ is true.

**Secret Generation:** Ultimately, the key, $\mathbf{K_A}$, is generated using information about the detected symbols, $\texttt{symb}$, and its source and is given as $\mathbf{K_A} = f(\texttt{Quant}(\|\mathbf{y_a}\|^2 \| \texttt{src} \oplus \texttt{symb}))$ where $f$ and $\texttt{Quant}$ are secret agreement and quantization function respectively [3]. Eve with maximum confusion ends with a key of 0.5 bit error rate which is equivalent to random guess.

## 2 CONCLUSION AND WORK IN PROGRESS

A new approach to facilitate secret key refreshment using physical layer anonymity of frequency oscillator drift was proposed. The problem of secret key generation is formulated under the framework of Bayesian hypothesis testing and the optimal error probabilities are being studied different channel models.

## REFERENCES

[1] 2016. Hands-on Rapid Prototyping Real-Time Wireless Systems with LabVIEW Communications. *National Instruments manual, http://www.ni.com/white-paper/52147/en/* (2016). https://doi.org/white-paper/52147/en/

[2] Adam C Polak and Dennis L Goeckel. 2015. Wireless device identification based on RF oscillator imperfections. *IEEE Transactions on Information Forensics and Security* 10, 12 (2015), 2492–2501.

[3] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy. 2013. Secret Key Extraction from Wireless Signal Strength in Real Environments. *IEEE Transactions on Mobile Computing* 12, 5 (May 2013), 917–930. https://doi.org/10.1109/TMC.2012.63

[4] Wei Xi, Xiang-Yang Li, Chen Qian, Jinsong Han, Shaojie Tang, Jizhong Zhao, and Kun Zhao. 2014. KEEP: Fast secret key extraction protocol for D2D communication. In *Quality of Service (IWQoS), 2014 IEEE 22nd International Symposium of*. IEEE, 350–359.