PHYSICAL LAYER AUTHENTICATION BASED ON CHANNEL RESPONSE TRACKING USING GAUSSIAN PROCESSES

Steven Van Vaerenbergh, Óscar González, Javier Vía, and Ignacio Santamaría

Department of Communications Engineering, University of Cantabria, Spain

ABSTRACT

Physical-layer authentication techniques exploit the unique properties of the wireless medium to enhance traditional higher-level authentication procedures. We propose to reduce the higher-level authentication overhead by using a state-of-the-art multi-target tracking technique based on Gaussian processes. The proposed technique has the additional advantage that it is capable of automatically learning the dynamics of the trusted user's channel response and the time-frequency fingerprint of intruders. Numerical simulations show very low intrusion rates, and an experimental validation using a wireless test bed with programmable radios demonstrates the technique's effectiveness.

Index Terms— wireless communications, physical-layer authentication, Gaussian processes, multi-target tracking

1. INTRODUCTION

Wireless communication systems have witnessed an impressive evolution during the past two decades, most significantly in terms of data rate and reliability. Nevertheless, an area that still leaves room for considerable improvement is security. The broadcast nature of the wireless channel facilitates both the interception of data, or *eavesdropping*, and intrusions, or *spoofing*. Traditional higher-layer security techniques are employed to prevent both types of attacks. Specifically, confidentiality techniques are employed to avoid eavesdropping, while authentication techniques aim to prevent spoofing.

We follow up on the idea that the very nature of the wireless medium, which may seem vulnerable to attacks at first, can be turned into an important advantage to complement traditional security methods [1, 2, 3]. In particular, the typical multipath environment in wireless communications guarantees that the response of the medium along any transmit-receive path is location-specific, and characterized by a particular frequency- and time-selectivity.

We will focus on the problem of authentication, for which several techniques have appeared in the literature. Yu et al. devised a framework to transmit authentication information concurrently by superposing a secret modulation on the waveform [2]. A different approach consists in authenticating the wireless transmitter by analyzing its channel response. For instance, Li et al. proposed a change-point detector to detect the presence of spoofing signals in [1], and a hypothesis test based on a realistic channel model was presented in [3].

This work was supported by MICINN (Spanish Ministry for Science and Innovation) under grants TEC2010-19545-C04-03 (COSIMA), CONSOLIDER-INGENIO 2010 CSD2008-00010 (COMONSENS) and FPU grant AP2009-1105.

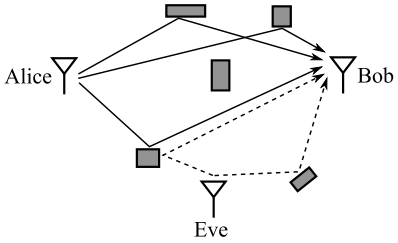

Fig. 1. Three agents in a multipath environment with multiple scattering surfaces.

In this paper, we propose a technique based on Gaussian processes (GPs) that solves two issues found in the current hypothesis-test based methods. First, they typically only serve as a detector for intruders, and whenever an intruder is detected they require the transmitter to re-authenticate itself, causing considerable overhead. And, second, the current PHY-layer authentication techniques are based on specific channel models and they require to know all involved parameters in order to perform correctly. The technique we propose is capable of tracking the dynamics of the channel by clustering the observations into trajectories, therefore reducing the need for higher-level authentication when intrusions are detected. Furthermore, it is non-parametric in the sense that it does not make any assumptions on the channel responses except for smoothness, and it is capable of automatically learning all parameters including the smoothness.

2. PROBLEM STATEMENT

Using the traditional terminology, we consider three different agents: Alice, Bob and Eve. These agents represent wireless transmitters or receivers that are located at different positions amid several scatterers, as depicted in Fig. 1. Alice is a legitimate transmitter who wishes to communicate with Bob, and

978-1-4799-2893-4/14/$31.00 ©2014 IEEE

Eve is a would-be intruder who transmits to Bob with the aim of impersonating Alice.

2.1. System model

We assume that Bob measures and stores the N most recent frequency responses of the channel between (a presumed) Alice and himself. The channel response at the n-th time slot, $\hat{\mathbf{h}}_n$, is stored as a $D \times 1$ vector of samples, each corresponding to a different frequency in the measurement bandwidth. A common example of this model would be that of an orthogonal frequency division multiplexing (OFDM) system where pilot symbols are transmitted over D different subcarriers. Bob stores a sliding window of N channel responses centered at time n, i.e. $\hat{\mathbf{h}}_i \; \forall i \in [n - \frac{N-1}{2}, \ldots, n + \frac{N-1}{2}]$. Based on the aforementioned set of channel responses, Bob has to decide whether the frame received at time n is coming from Alice or Eve. Commonly, received frames will be coming from Alice and, thus, they can be modeled as

$$\hat{\mathbf{h}}_n = \mathbf{h}_n^{(AB)} + \mathbf{w}_n^{(AB)}, \tag{1}$$

where $\mathbf{h}_n^{(AB)}$ denotes the actual channel response between Alice and Bob, which will be time-variant and frequency-selective, and $\mathbf{w}_n^{(AB)}$ is the unavoidable estimation error vector which accounts for any spurious effect such thermal noise, non-linearities, etc. We recall that entries of samples $\hat{\mathbf{h}}_n$ are complex variables containing estimates of both channel amplitude and phase. The estimated channel phase is the additive combination of phases from two different sources: the actual channel phase and an arbitrary oscillator phase. Channel phase will typically change smoothly over time, but the oscillator phase can take independent values for each n. Therefore, Bob will find it difficult to discriminate between both of them and should restrict his attention to channel magnitudes instead of complex gains. Hereinafter, we will denote by $\hat{\mathbf{h}}_n$ the vector containing the amplitudes of the estimated channel response coefficients.

Given the malicious nature of Eve, she will try to perform an attack by sending a forged message to Bob. We assume that Eve knows the modulation scheme, the frequency/time statistics of the channel between Alice and Bob and the details of the channel estimation and authentication technique employed by Bob. Our assumptions are, therefore, conservative and provide worst-case scenarios. It is well known that channel responses decorrelate rapidly in space, that is, two transmit-receive paths are decorrelated from each other if the paths are separated by more than a radio frequency (RF) wavelength. For that reason, Eve will not be able to know the exact channel response of the path separating Alice and Bob but she will be able to estimate the propagation environment time and frequency characteristics.

Taking again a conservative viewpoint, we will assume Eve can potentially forge, by pre-distorting her signal, any channel response with the same characteristics as the channel between Alice and Bob. This may not be possible in practice, for instance due to limitations on Eve's transmission power. The attack strategy of Eve will consist in transmitting as many different frames per time unit as possible, emulating a high number of different channel responses. For each of these frames, Bob estimates a channel response that may be written as

$$\hat{\mathbf{h}}_n = \mathbf{h}_n^{(EB)} + \mathbf{w}_n^{(EB)} \tag{2}$$

where $\mathbf{w}_n^{(EB)}$ is the estimation error and $\mathbf{h}_n^{(EB)}$ is the channel response crafted by Eve, i.e. not the actual response of the Eve-Bob channel.

3. CHANNEL TRACKING THROUGH OMGP

In [1] a simple change-point detector was proposed to detect interruptions in the state of the wireless channel, quantified as

$$\eta_n = \frac{\|\hat{\mathbf{h}}_n - \hat{\mathbf{h}}_{n-1}\|}{\|\hat{\mathbf{h}}_{n-1}\|}. \tag{3}$$

If, during the transmission of Alice, a spike in η_n is detected, it is likely that another device is using the wireless channel with the possible intention of spoofing Alice. At this point Bob may ask Alice to re-authenticate herself by traditional methods in order to resume the transmission. However, if at time $n+1$ Alice does not re-authenticate herself, the detector does not allow to determine who is transmitting. In [3] the change-point detector from Eq. (3) was extended to a hypothesis test for authentication that is capable of incorporating the channel model whenever its parameters are known. Nevertheless, this approach faces the same limitation.

In order to circumvent this problem, we propose to track the changes in the channel response rather than to rely only on the last estimate of the trusted Alice-Bob channel. As a result, when Eve is detected at time instant n it is still possible to recognize Alice at time instant $n+1$ without Alice having to re-authenticate herself, thereby causing less overhead.

The tracking-based detector takes the following general form:

$$\gamma_n = \|\hat{\mathbf{h}}_n - \hat{\mathbf{h}}_n^{(AB)}\|, \tag{4}$$

where $\hat{\mathbf{h}}_n^{(AB)}$ represents the response of the channel between Alice and Bob at time n, as estimated by the tracking algorithm.

In this work we use the recently-proposed Overlapping Mixture of Gaussian Processes (OMGP) multi-target tracking algorithm from [4] to distinguish Alice's and Eve's transmissions. We summarize its main characteristics below.

3.1. Trajectories as Gaussian processes

The OMGP model casts trajectories as Gaussian processes, which are state-of-the-art Bayesian models for regression and

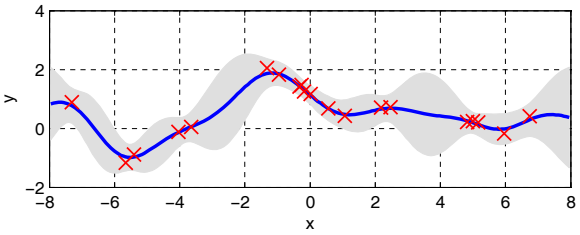

Fig. 2. GP regression on the noisy data marked by the red crosses. The inferred latent function is shown as the blue curve, and the grey area marks the 95% confidence interval.

classification [5, 6]. Given a set of N inputs and their corresponding outputs, $\mathcal{D} \equiv \{\mathbf{x}_i, y_i\}_{i=1}^N$, the Gaussian process regression model assumes that the observations can be modeled as

$$y = f(\mathbf{x}) + \epsilon, \tag{5}$$

where $f(\mathbf{x})$ is an unobservable latent function and ϵ represents zero-mean Gaussian noise. In order to perform Bayesian inference a GP prior is placed over the latent function, chosen as a zero-mean GP with covariance function $k(\mathbf{x}_i, \mathbf{x}_j)$. The use of a GP prior implies that the prior joint distribution of the vector $[f(\mathbf{x}_1), f(\mathbf{x}_2), \ldots, f(\mathbf{x}_n)]^\top$ is a zero-mean multivariate Gaussian with covariance matrix $\mathbf{K}$, which has elements $\mathbf{K}_{ij} = k(\mathbf{x}_i, \mathbf{x}_j)$.

The covariance function $k(\mathbf{x}_i, \mathbf{x}_j)$ specifies the degree of coupling between y_i and y_j, and it encodes the properties of the GP such as power level, smoothness, etc. One of the best-known covariance functions is the squared exponential kernel. It has the form of an unnormalized Gaussian, $k(\mathbf{x}_i, \mathbf{x}_j) = \sigma_0^2 \exp\left(-\|\mathbf{x}_i - \mathbf{x}_j\|^2/l\right)$, and depends on the signal power σ_0^2 and the length-scale l, which controls how fast the correlation between outputs decays as the separation along the inputs grows. We will collectively refer to all kernel parameters as $\boldsymbol{\theta}$. Many different covariance functions can be plugged into the GP regression framework. For instance, in the experiments of Section 4 we will see that it may be useful to use a noise-like covariance to model Eve's channel in case she performs random attacks, as opposed to Alice's smooth trajectory.

3.2. Data association without combinatorial explosion

Given a set of observations that represent the positions of a number of moving targets in a multi-target tracking setting, typically cars or airplanes, data association consists of inferring which observations correspond to the same target [7]. While data association is typically performed online, the results can be significantly improved by postponing decisions until enough information is available to exclude ambiguities. Nevertheless, this causes the number of possible trajectories to grow exponentially.

The OMGP model allows to avoid such combinatorial explosions, and to "cluster" observations into groups that represents trajectories. It assumes that there exist M different multi-dimensional trajectories, each of which are described by D latent functions $\{f_d^{(m)}(\mathbf{x})\}_{m=1,d=1}^{M,D}$. In our case, D is the number of subcarriers, and M is the number of targets, which is typically 2 to represent Alice and Eve, but it may be higher when more intruders are sought. The OMGP model assumes that each observation is produced by evaluating one of these functions at the corresponding input and by adding Gaussian noise to it. The association between samples and latent functions is determined by the $N \times M$ binary indicator matrix $\mathbf{Z}$: Entry $[\mathbf{Z}]_{nm}$ being non-zero specifies that n-th data point was generated using trajectory m. Only one non-zero entry per row is allowed in $\mathbf{Z}$.

All the outputs can be collected in a single matrix $\mathbf{Y} = [\mathbf{y}_1 \ldots \mathbf{y}_D]$ and all the latent functions of trajectory m in a single matrix $\mathbf{F}^{(m)} = [\mathbf{f}_1^{(m)} \ldots \mathbf{f}_D^{(m)}]$. The complete set of latent functions is denoted as $\{\mathbf{F}^{(m)}\}$. The likelihood of the OMGP model is

$$p(\mathbf{Y}|\{\mathbf{F}^{(m)}\}, \mathbf{Z}) = \prod_{n,m,d} \mathcal{N}([\mathbf{Y}]_{nd}|[\mathbf{F}^{(m)}]_{nd}, \sigma^2)^{[\mathbf{Z}]_{nm}}. \tag{6}$$

The posterior distribution $p(\mathbf{Z}, \{\mathbf{F}^{(m)}\}|\mathbf{X}, \mathbf{Y})$ is obtained by placing priors on the latent variables. Since it cannot be computed analytically, the OMGP algorithm uses an efficient variational approximation technique. Details can be found [4].

In our setup, the measured channels $\hat{\mathbf{h}}_n$ constitute the rows of $\mathbf{Y}$, and the rows of $\mathbf{F}^{(1)}$ and $\mathbf{F}^{(2)}$ correspond to the true, unobservable channel responses $\mathbf{h}_n^{(AB)}$ and $\mathbf{h}_n^{(EB)}$, respectively. The time instants at which the channels are estimated are collected in $\mathbf{X}$.

3.3. Automatic parameter learning

The OMGP algorithm does not require exact information about the tracking environment. Rather, it can *learn* all involved parameters from the provided data by maximizing the likelihood of the OMGP model. An expectation maximization (EM) algorithm to determine the involved parameters is detailed in [4].

4. EXPERIMENTS

4.1. Simulation

The fading dispersive channel between Alice and Bob can be characterized by its low-pass equivalent impulse response $h(t, \tau)$ where τ is the propagation delay and t denotes absolute time. Given $h(t, \tau)$, the power-delay profile (PDP) represents the mean power of the multipath component at delay τ, $P(t, \tau) = E[|h(t, \tau)|^2]$. In our simulations we will consider a Rayleigh fading channel with the classic one-sided exponential PDP [8]:

$$P(t, \tau) = \frac{1}{\sigma_T} \exp(-\frac{\tau - t}{\sigma_T}) \quad \text{for } \tau - t \geq 0, \tag{7}$$

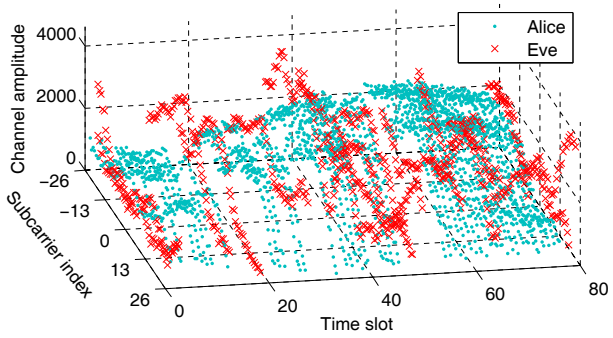

Fig. 3. Simulated channel responses at different time slots.

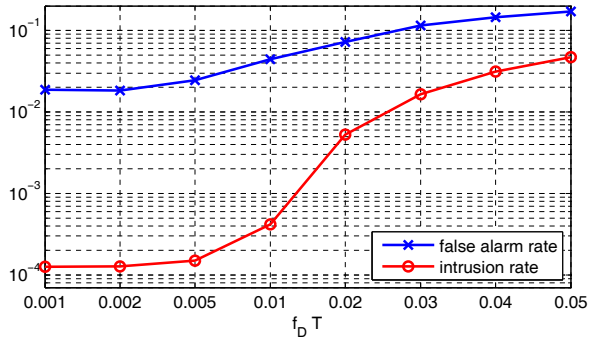

Fig. 4. Results for the simulated authentication scenarios.

where the frequency selectivity of the channel is parametrized by the root mean square (RMS) delay spread σ_T, here chosen as $\sigma_T = 1$. Similarly, in order to model the time selectivity of the channel we use the well-known Jakes model [9] which allows us to parametrize the time-variability of the channel by means of a single parameter f_D denoting the Doppler frequency. Note that Bob does not know any of these channel parameters. Estimation errors have been modeled as zero-mean real Gaussian i.i.d random variables with variance σ. The time instants on which Alice transmits are not uniformly spaced but determined by a Markov chain, while Eve is set to attack at random time instants. An example scenario with the data to track is shown in Fig. 3.

We apply the OMGP tracking algorithm on these data. For Alice we choose a squared exponential covariance as her channel will undergo smooth changes, and the smoothness is determined automatically by the OMGP algorithm. For Eve we choose a noise-like covariance (implying a diagonal covariance matrix), in accordance with her attack strategy. The tracking algorithm uses a buffer of $N = 50$ samples to make a decision on a single observation. The false alarm rates and rates of successful intrusions for different relative Doppler spreads, $f_D T$, can be found in Fig. 4.

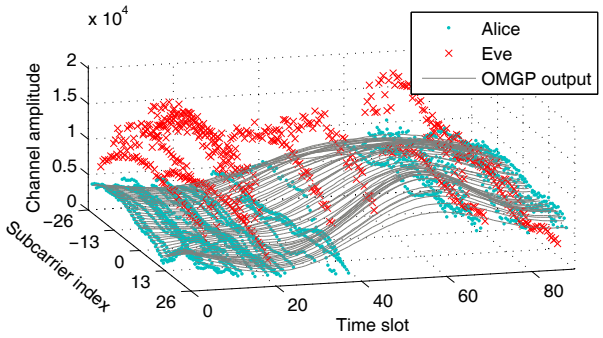

Fig. 5. Observed channel response coefficients, for Alice and Eve, and inferred trajectories for Alice, using real-world channel data.

4.2. Experimental validation

Any proposed PHY-layer authentication method requires the radio equipment to provide higher layers with the estimated channel amplitudes. In our experiments we have used the GTAS MIMO test bed[1] to transmit fully compliant 802.11a frames from two nodes representing Alice and Eve and estimate channel responses at Bob's receiver end. Measurements were carried out in an indoor environment at a center frequency of 5.6 GHz where Alice and Eve were one meter apart from each other and five meters apart from Bob. Additional details on the test bed and measurement scenario can be found in [10, 11].

Our measurements show that in spite of the proximity of Alice and Eve, the spatial correlation between their multicarrier channel responses is rather low and should be enough for discrimination. This validates our space correlation assumption. Furthermore, we observed time and frequency characteristics which are similar to those assumed in Section 4.1, thus validating our simulation model assumptions. As an example, Figure 5 shows the retrieved trajectories of the proposed method under real-world channel conditions.

5. CONCLUSIONS

We have proposed a methodology for physical-layer authentication that requires less overhead from higher-level authentication methods compared to the currently proposed techniques. Our approach is based on a GP tracking algorithm that has the additional advantage that it is capable of automatically learning the parameters of the trajectories.

We have presented simulation results that show very low intrusion rates, and we have performed an experimental validation of our approach using a wireless test bed with programmable radios.

[1]The GTAS MIMO test bed is a MIMO experimentation test bed which is openly available to researchers willing to conduct their own PHY-layer experiments through an online interface.

6. REFERENCES

[1] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *Proceedings of the 5th ACM workshop on Wireless security*. ACM, 2006, pp. 33–42.

[2] P. L. Yu, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *Information Forensics and Security, IEEE Transactions on*, vol. 3, no. 1, pp. 38–51, 2008.

[3] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2571–2579, 2008.

[4] M. Lázaro-Gredilla, S. Van Vaerenbergh, and N. D. Lawrence, "Overlapping mixtures of Gaussian processes for the data association problem," *Pattern Recognition*, vol. 45, no. 4, pp. 1386–1395, 2012.

[5] C. E. Rasmussen and C. K. I. Williams, *Gaussian Processes for Machine Learning*, MIT Press, 2006.

[6] F. Pérez-Cruz, S. Van Vaerenbergh, J. J. Murillo-Fuentes, M. Lázaro-Gredilla, and I. Santamaría, "Gaussian processes for nonlinear signal processing: An overview of recent advances," *Signal Processing Magazine, IEEE*, vol. 30, no. 4, pp. 40–50, 2013.

[7] I. J. Cox, "A review of statistical data association techniques for motion correspondence," *International Journal of Computer Vision*, vol. 10, no. 1, pp. 53–66, 1993.

[8] A. A. Saleh and R. A. Valenzuela, "A statistical model for indoor multipath propagation," *IEEE Journal on Selected Areas in Communications*, vol. SAC-5, no. 2, pp. 128–137, 1987.

[9] W. C. Jakes, Ed., *Microwave mobile communications*, IEEE Press, New York, second edition, 1994.

[10] L. Vielva, J. Vía, J. Gutiérrez, Ó. González, J. Ibáñez, and I. Santamaría, "Building a web platform for learning advanced digital communications using a MIMO testbed," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2010)*, Dallas, USA, March 2010.

[11] J. Gutiérrez, Ó. González, J. Pérez, D. Ramírez, L. Vielva, J. Ibáñez, and I. Santamaría, "Frequency-domain methodology for measuring MIMO channels using a generic test bed," *IEEE Transactions on Instrumentation and Measurement*, vol. 60, no. 3, pp. 827–838, 2011.