Feature-Based Multi-User Authentication for Parallel Uplink Transmissions

(Invited Paper)

H. Forssell, R. Thobaben, J. Gross, and M. Skoglund
KTH Royal Institute of Technology and ACCESS Linnaeus Centre,
SE-100 44 Stockholm, Sweden
E-mail: {hefo, ragnart, jamesgr, skoglund}@kth.se

***Abstract*—We study a multi-user up-link scenario where an attacker tries to impersonate the legitimate transmitters. We present a new framework for deriving *a posteriori* attack probabilities from the channel observations at the access point, which enables fast intrusion detection and authentication at the physical layer and can be exploited to reduce the security overhead by offloading higher-layer authentication schemes. This is highly relevant for delay-sensitive applications that are targeted in 5G where the security overhead may limit the real-time performance. We take a factor-graph approach that can easily be extended to take into account other features, channel models, and radio access schemes. While related works only consider single-link scenarios, the multi-user approach in this paper allows us to exploit the cross-channel correlation of the large-scale fading parameters that is due to the propagation environment for improving the detection performance. As numerical results show, especially for slowly changing channels with high correlation our approach provides significant performance gains.**

I. Introduction

The broadcast nature of the wireless medium makes wireless communications vulnerable against various attacks. Among the possible attacks, impersonation attacks are of special interest, since if successful, they open up for follow-up attacks with severe consequences [1]. Traditional authentication schemes that are based on pre-shared authentication keys or pairs of public/private keys provide a good protection against intrusion; however, they add a significant security overhead to the system. In new applications that are targeted in 5G (e.g., industrial IoT, smart cities), where low-complexity embedded devices carry out sensing and actuation tasks under stringent latency constraints, this security overhead often turns into a problem as it affects the real-time performance of the system.

In this paper, we study alternative means to identify wireless transmitters in order to offload higher layer security schemes, and hence, to reduce the security overhead while still ensuring high reliability in authentication. We provide a framework for deriving *a posteriori* attack probabilities from the channel observations by utilizing appropriate channel models. The *a posteriori* attack probabilities can then be used to set up a physical-layer authentication scheme or to assist higher-layer authentication schemes with intrusion detection at the physical layer. Our approach shares some similarities with recent work on feature-based physical-layer authentication, which uses imperfections of the transmitted signal and characteristic properties of the communication channel for identification and authentication. For example, feature-based authentication in multiple-antenna systems was investigated in, e.g., [2], [3], and the work in [2] also utilizes time-variant channel models for the channel frequency response. Tracking of the channel responses of multiple users using multiple-target tracking algorithms for Gaussian processes has been studied in [4].

This work is supported in part by the Swedish Civil Con- tingencies Agency, MSB, through the CERCES project.

In this paper, we provide a generic framework for deriving *a posteriori* attack probabilities from factor graphs. Our framework can easily be extended in order to take into account additional features, other channel models and radio access technologies, as well as data models for bad-data detection. It is compatible with iterative receiver architectures that are expected to be used in 5G. While related works only consider single-link scenarios, we consider a multi-user uplink scenario and exploit the fact that the slowly changing large-scale fading parameters are correlated due to the propagation environment (e.g., reflecting objects) such that changes in the environment (e.g., moving objects) affect multiple channels at the same time. Numerical results show that gains in the detection performance of up to one order of magnitude can be obtained for slowly changing channels with high correlation.

The remainder of this paper is organized as follows: Section II summarizes the system model and assumptions. In Section III, we present our framework for deriving the *a posteriori* attack probabilities. Numerical results are presented in Section IV, and our conclusions are summarized in Section V.

II. System Model and Assumptions

We consider uplink transmissions from a set of M devices D_i, $i \in \{1, \ldots, M\}$, to an access point (AP) and assume that an attacker, Eve, is present that with probability p_A tries to impersonate the legitimate devices. Motivated by the target applications mentioned in the introduction, we consider a static scenario where the devices and the AP are deployed in fixed locations and possibly in a public environment. For ease of presentation, we consider a time division multiple access scheme where the medium access is coordinated by the AP. Every frame spans the duration T_f and is split into two phases of lengths T_b and T_{UL}. In the first phase, the AP broadcasts a beacon containing scheduling information as well as training data for channel estimation at the devices. In the second phase, the devices enter the channel as specified by the AP.

Throughout this paper, k and i denote the frame index and the index for enumerating transmissions within the frames,

respectively. We introduce the random vector $\mathbf{T}^{(k)}$ to identify the schedule in frame k, and assume that the i-th component $T_i^{(k)} \in \{D_1, \ldots, D_M\}$ identifies the device that is granted access in the i-th time slot in frame k. We consider a cyclic-prefix OFDM system with N_c carriers where the channel observation in frequency domain at the AP for the i-th transmission within the k-th frame (after matched filtering, sampling with symbol duration T_s, and OFDM demodulation) is given by

$$\mathbf{Y}_i^{(k)} = \mathbf{X}_i^{(k)} \odot \mathbf{H}_i^{(k)} + \mathbf{W}_i^{(k)}, \tag{1}$$

where the length-N_c random vectors $\mathbf{X}_i^{(k)}$, $\mathbf{H}_i^{(k)}$, and $\mathbf{W}_i^{(k)}$ denote the vector of transmitted symbols, the channel frequency response, and the additive white Gaussian noise at the receiver, respectively, and $\odot$ denotes the element-wise multiplication. We assume that every transmission $\mathbf{X}_i^{(k)}$ includes an identifier for the transmitter, pilot symbols that allow for coherent detection at the AP, and data. We assume furthermore that channel coding rates at the transmitters are carefully set (e.g., by utilizing the training symbols in the beacon from the AP) such that decoding errors at the AP are negligible.

We adopt the wide-sense-stationary uncorrelated scattering (WSSUS) channel model and describe the channel impulse response as a zero-mean complex Gaussian random vector with independent components where the variances follow the power delay profile $\mathbf{P}$. A WSSUS model of the time variation of the impulse response is given by a first-order Markov model with Gaussian process noise of zero mean and covariance $\mathrm{diag}\{\mathbf{P}\}$ and correlation coefficient $\alpha_{D_j}^{(k)}$, which for a separable scattering function is related to the Doppler spectrum. Hence, the frequency response $\mathbf{H}_i^{(k)}$ is a zero-mean complex Gaussian random vector with covariance matrix $\mathbf{C_H} = \mathbf{U} \cdot \mathrm{diag}\{\mathbf{P}\} \cdot \mathbf{U}^H$, where $\mathbf{U}$ is the $N_c \times N_c$ Fourier transform matrix and we assume that $\mathbf{P}$ is extended to length N_c by zero-padding. The temporal correlation of the frequency response is then described by the AR process:

$$\mathbf{H}_{D_j}^{(k)} = \alpha_{D_j}^{(k)} \mathbf{H}_{D_j}^{(k-1)} + \sqrt{(1 - {\alpha_{D_j}^{(k)}}^2)} \mathbf{Z}_{D_j}^{(k)}, \tag{2}$$

where $\mathbf{Z}_{D_j}^{(k)}$ is the zero-mean complex Gaussian process noise with covariance matrix $\mathbf{C_Z} = \mathbf{C_H}$. We assume that the realizations of the channels are independent across the users; however, since the correlation coefficients are determined by movements and changes in the environment through the Doppler spectrum, we assume that correlation coefficients are time-variant, correlated in time and across the channels of the devices, and conditionally independent given the state of the propagation environment $S_{\text{Prop}}^{(k)}$.

For our model, different attack scenarios are possible:

Scenario 1: If guard intervalls between successive transmissions are sufficiently long (e.g., in order to compensate for lack of synchronization), Eve can place a transmission between two scheduled transmissions. As a consequence the AP will observe $N > M$ transmissions.

Scenario 2: Eve enters the time slot of a scheduled device such that the AP will observe $N = M$ transmissions. In the case where the scheduled device and Eve transmit simultaneously, Eve needs to ensure that her transmission will be correctly decoded by the AP in order to be successful; i.e., Eve needs to communicate either from a favourable location close to the AP or overpower the concurrent transmission of the scheduled device. As a consequence the AP will observe a significant increase in received signal power.

Scenario 3: Eve enters the time slot of a scheduled device but physically manipulates the scheduled device in order to suppress its transmission.

Since the increased number of received transmissions in Scenario 1 and the large fluctuations in the received power that can be expected in Scenario 2 give a clear indication that an attack is ongoing, we assume that these scenarios can easily be detected. We therefore focus on Scenario 3 in the remainder of this paper, for which no obvious indications for an attack are available. However, we note that our approach can easily be extended to also include the Scenarios 1 and 2.

III. Feature-Based Multi-User Authentication and Intrusion Detection

We now present a new approach to feature-based multi-user authentication. Ultimately, we are interested in deriving the *a posteriori* attack probability $\Pr(\text{Eve} \,|\mathbf{X}^{([1,k])}, \mathbf{Y}^{([1,k])})$ under the assumptions made in the previous section. Even though it is possible to describe the evolution of all involved random processes by a hidden Markov model and to derive the *a posteriori* attack probability from this model, this approach is not very practical since it requires deriving marginal distributions over all combinations of all realizations of all random variables. Instead, we model the underlying problem by a factor graph and derive an efficient solution as an approximation of the sum-product algorithm (see, e.g., [5]).

A. Factor Graph

In order to keep the notation compact, let $\mathbf{Y}^{(k)} = [\mathbf{Y}_1^{(k)}, \ldots, \mathbf{Y}_N^{(k)}]$ and $\mathbf{Y}^{([1,k])} = [\mathbf{Y}^{(1)}, \ldots, \mathbf{Y}^{(k)}]$, where N is the number of transmissions observed by the AP during the k-th frame. Let $\mathbf{X}^{(k)}$ and $\mathbf{X}^{([1,k])}$ be defined similarly. We introduce the random variable $A_i^{(k)} \in \{D_1, \ldots, D_M, \text{Eve}\}$ to indicate which node causes the channel observation $\mathbf{Y}_i^{(k)}$. Since we assume that the transmitted codewords $\mathbf{X}_i^{(k)}$ have already been decoded they are treated as observations as well.

The factor graph that we use in this paper is shown in Fig. 1. It is a bipartite graph consisting of variable nodes (VN, circles in Fig. 1) and function nodes (FN, black squares) that are connected by edges. Every VN represents a random variable, and every FN corresponds to a specific (conditional and/or joint) density of the connected random variables that is obtained as a factor when factorizing the joint density of all involved random variables. The factor graph in Fig. 1 is derived under the assumption that (i) Scenario 3 is considered and (ii) the schedule $\mathbf{T}^{(k)}$ is fixed and does not change over time. It is interesting to note that for a given state of the propagation environment $S_{\text{Prop}}^{(k)}$, the realizations of the correlation parameters $\alpha_i^{(k)}$ are independent across the channel uses $i \in \{1, \ldots, N\}$, and hence the factor graph in Fig. 1

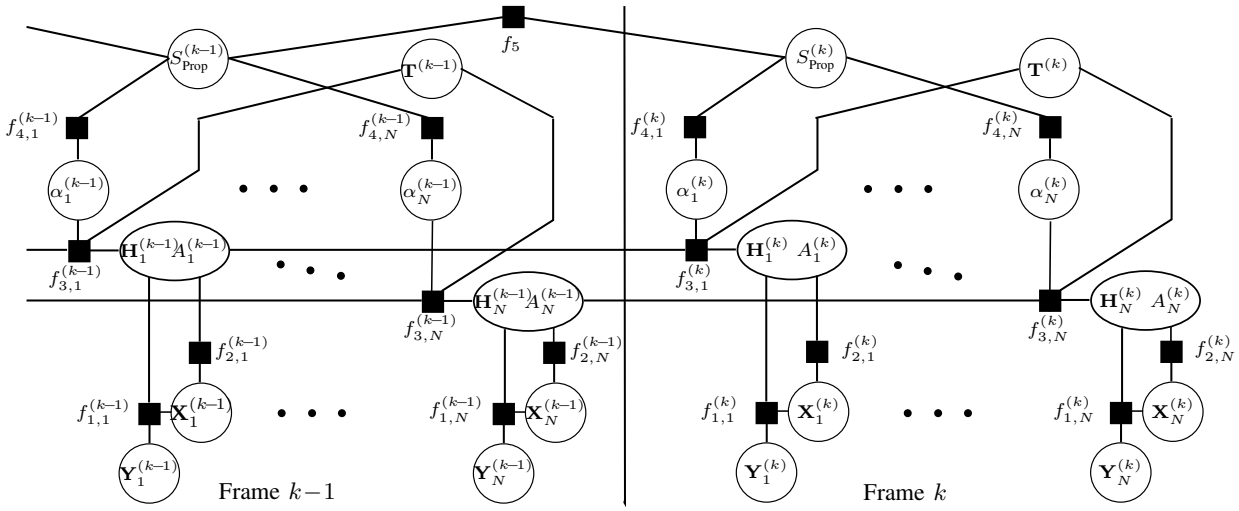

Fig. 1: Factor graph describing the structure of the underlying detection problem.

shows the structure of N parallel hidden Markov chains that are coupled via the state variable $S_{\text{Prop}}^{(k)}$.

The FNs in Fig. 1 are now defined as follows. The first factor takes into account the channel model from (1),

$$f_{1,i}^{(k)} = p(\mathbf{Y}_i^{(k)} = \mathbf{y} | \mathbf{X}_i^{(k)} = \mathbf{x}, \mathbf{H}_i^{(k)} = \mathbf{h}) = p(\mathbf{W}_i^{(k)} = \mathbf{y} - \mathbf{h} \odot \mathbf{x}),$$

The factor $f_{2,i}^{(k)}$ utilizes that every codeword $\mathbf{X}_i^{(k)}$ carries an identifier $\text{ID}(\mathbf{X}_i^{(k)})$ for the transmitter. Assuming that all legitimate devices identify themselves correctly, we have

$$\begin{aligned} f_{2,i}^{(k)} &= p(\mathbf{X}_i^{(k)} = \mathbf{x} | A_i^{(k)} = a) \\ &= \begin{cases} 1, & a = \text{ID}(\mathbf{x}) \text{ and } a \neq \text{Eve}, \\ 1/M, & a = \text{Eve}, \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

The third factor incorporates the correlation model for the channel response from (2) and the schedule $\mathbf{T}^{(k)}$. Since the model is changing depending on the hypotheses of $A_i^{(k)}$ and $A_i^{(k-1)}$, we distinguish the following cases:

$$\begin{aligned} f_{3,i}^{(k)} &= p(\mathbf{H}_i^{(k)} = \mathbf{h}, A_i^{(k)} = a | \ldots \\ &\qquad \mathbf{H}_i^{(k-1)} = \mathbf{h}', A_i^{(k-1)} = a', \alpha_i^{(k)} = \alpha, \mathbf{T}^{(k)} = \mathbf{t}) = \\ &\begin{cases} p(\mathbf{Z}_i^{(k)} = \frac{\mathbf{h} - \alpha \mathbf{h}'}{\sqrt{1-\alpha^2}}) \frac{1-p_A}{(1-\alpha^2)^{N_c}}, & a' = a = t_i, \\ p(\mathbf{Z}_i^{(k)} = \mathbf{h}) \cdot p_A & a' = t_i \text{ and } a = \text{Eve}, \\ p(\mathbf{Z}_i^{(k)} = \mathbf{h}) \cdot (1 - p_A) & a' = \text{Eve and } a = t_i, \\ p(\mathbf{Z}_i^{(k)} = \frac{\mathbf{h} - \alpha \mathbf{h}'}{\sqrt{1-\alpha^2}}) \frac{p_A}{(1-\alpha^2)^{N_c}}, & a' = a = \text{Eve}, \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \quad (3)$$

The term $(1-\alpha^2)^{N_c}$ is a normalization factor that takes into account the scaling of the impulse response in the first and fourth case. We also assume that Eve mimics the behaviour of a legitimate user and keeps its antenna at the same position when attacking the same node in two successive time frames. However, it is straight forward to extend the last case to describe a different behaviour including attacker models with memory. The two remaining factors $f_{4,i}$ and f_5 describe the mapping of the state of the environment to the correlation coefficients $\alpha_i^{(k)}$ and the temporal correlation of the state of the environment, respectively. Due to page constraints, we only consider the extreme case where all correlation coefficients $\alpha_i^{(k)}$ take on the same value $\alpha^{(k)}$ and neglect their temporal correlation. That is, $S_{\text{Prop}}^{(k)} = \alpha^{(k)}$, $f_{4,i} = \delta_0(\alpha^{(k)} - \alpha_i^{(k)})$, and $f_5 = p(\alpha^{(k)})$, with $p(\alpha^{(k)}) = \text{Unif}([\alpha_{\min}, 1])$, where $\alpha_{\min}$ is the minimum correlation coefficient, which is related to T_f and the maximum speed of objects observed in the environment $v_{\max}$ through the Doppler spectrum.

B. Sum-Product Algorithm and Message Schedule

For every VN in the graph, the *a posteriori* distribution can be approximated by running the sum-product message-passing algorithm[1] [5]. VNs and FNs exchange messages along the connecting edges following a prescribed schedule. For a given edge, each message characterizes the density of the connected VN. Assume that a VN V_i is connected to FNs $f_1, \ldots, f_F$. Then, the message $M_{V_i \to f_j}(x)$ from V_i along the edge to f_j is obtained as the product of all incoming messages at V_i except the message from f_j [5]:

$$M_{V_i \to f_j}(x) = \prod_{k=1, k \neq j}^{F} M_{f_k \to V_i}(x).$$

On the other hand, let a FN f_i be connected to VNs $V_1, \ldots, V_F$ (i.e., f_i is a function of $V_1, \ldots, V_F$). Then, the message from f_i to V_j is obtained as the marginal distribution[2] [5]

$$\begin{aligned} M_{f_i \to V_j}(v_j) = \int \ldots \int f(v_1, \ldots, v_F) \cdot M_{V_1 \to f_i}(v_1) \cdot \ldots \\ \cdot M_{V_F \to f_i}(v_F) \; dv_1 \ldots dv_{j-1} dv_{j+1} \ldots dv_F. \end{aligned} \quad (5)$$

Using this notation, we can approximate the desired *a posteriori* attack probability as

$$\begin{aligned} &\Pr(A_i^{(k)} = \text{Eve} | \mathbf{X}^{([1,k])}, \mathbf{Y}^{([1,k])}, \mathbf{T}^{([1,k])}) \\ &\qquad = \int M_{(\mathbf{H}_i^{(k)}, A_i^{(k)}) \to f_{3,i}^{(k+1)}}(\mathbf{h}, \text{Eve}) d\mathbf{h}, \end{aligned} \quad (6)$$

[1]Note that the sum-product algorithm only provides the exact *a posteriori* probabilities if it is applied to graphs without loops.

[2]For discrete random variables, the integrals are replaced by summations.

$$I_i(\alpha,a,a') = \int_{\mathcal{H}} M_{(\mathbf{H}_i^{(k)},A_i^{(k)})\to f_{3,i}^{(k)}}(\mathbf{h},a) \int_{\mathcal{H}} f_{3,i}^{(k)}(\mathbf{h},\mathbf{h}',a,a',\alpha) M_{(\mathbf{H}_i^{(k-1)},A_i^{(k-1)})\to f_{3,i}^{(k)}}(\mathbf{h}',a') d\mathbf{h}' d\mathbf{h} \tag{4}$$

and the main goal of the sum-product algorithm is now to calculate the message $M_{(\mathbf{H}_i^{(k)},A_i^{(k)})\to f_{3,i}^{(k+1)}}$.

Since the messages $M_{(\mathbf{H}_i^{(k-1)},A_i^{(k-1)})\to f_{3,i}^{(k)}}$ are already available from the derivations of the previous frame $k-1$, it is sufficient to restrict the message schedule to frame k. Note that for fixed messages $M_{(\mathbf{H}_i^{(k-1)},A_i^{(k-1)})\to f_{3,i}^{(k)}}$ the part of the factor graph that corresponds to frame k forms a tree. That is, it is sufficient to propagate the information from the observations $\mathbf{X}_i^{(k)}$, $\mathbf{Y}_i^{(k)}$ through the graph to the VN $S_{\text{Prop}}^{(k)}$ and back from the VN $S_{\text{Prop}}^{(k)}$ to the VNs $(\mathbf{H}_i^{(k-1)}, A_i^{(k-1)})$. Further iterations are only required if new information from future frames $k' > k$ is fed back. The proposed schedule can now be summarized in three steps: In a first step, for every time slot i, we derive a marginal distribution for the correlation coefficients $\alpha_i^{(k)}$ given by the message $M_{f_{3,i}^{(k)}\to\alpha_i^{(k)}}$ that is passed upwards to the VN $S_{\text{Prop}}^{(k)}$. In a second step, updated densities that carry the information provided from the other time slots are passed downwards to the FNs $f_{3,i}^{(k)}$, which allows us now to recursively derive the desired messages $M_{(\mathbf{H}_i^{(k)},A_i^{(k)})\to f_{3,i}^{(k+1)}}$ from the previously derived messages $M_{(\mathbf{H}_i^{(k-1)},A_i^{(k-1)})\to f_{3,i}^{(k)}}$.

C. Approximations and Implementation

So far, we have established a generic framework that allows us to derive the *a posteriori* attack probabilities. However, the message calculation in the FNs $f_{3,i}^{(k)}$ involves the marginalization over the distributions of the frequency response $\mathbf{H}_i^{(k-1)}$ and the correlation coefficients $\alpha_i^{(k)}$. To reduce the complexity, we consider two approximations: (i) we simplify parts of the sum-product algorithm to Gaussian message passing, and (ii) we use the maximum *a posteriori* (MAP) estimates of the correlation coefficients instead of their densities.

a) Gaussian Messages Passing: Since our factor graph includes the Gaussian models (1) and (2), it is natural to model messages that are densities of the frequency response by Gaussian distributions that are parametrized by their mean and covariance matrices. This approach accurately describes the messages $M_{f_{1,i}\to\mathbf{H}_i^{(k)}}$, and it follows that the messages $M_{(\mathbf{H}_i^{(k-1)},A_i^{(k-1)})\to f_{3,i}^{(k)}}$ have the form

$$M_{(\mathbf{H}_i^{(k-1)},A_i^{(k-1)})\to f_{3,i}^{(k)}}(\mathbf{h},a) = \begin{cases} (1-c_i^{(k)})\cdot CN(\mathbf{h}|\mathbf{m}_{D_i},\mathbf{C}_{\mathbf{D_i}}), & a = D_i, \\ c_i^{(k)}\cdot CN(\mathbf{h}|\mathbf{m}_{\text{Eve}},\mathbf{C}_{\text{Eve}}), & a = \text{Eve}, \end{cases} \tag{7}$$

where $CN(\mathbf{h}|\mathbf{m},\mathbf{C})$ denotes a complex Gaussian distribution with mean vector $\mathbf{m}$ and covariance matrix $\mathbf{C}$ evaluated in $\mathbf{h}$. Comparing (7) with (6), we can conclude that the quantity $c_i^{(k)}$ equals the *a posteriori* attack probability.

b) Estimation of Correlation Coefficients: Under the assumptions from above, the *a posteriori* density of the global correlation coefficient $\alpha^{(k)}$ is given by the product of the *a priori* distribution $f_5(\alpha^{(k)})$ and the densities $M_{f_{3,i}^{(k)}\to\alpha_i^{(k)}}(\alpha^{(k)})$. Let the scheduled user in time slot i be D_i and $\mathcal{A} = \{D_i, \text{Eve}\}$; then the message from $f_{3,i}^{(k)}$ to $\alpha_i^{(k)}$ is the marginal over the four possible transitions from $A_i^{(k-1)} \in \mathcal{A}$ to $A_i^{(k)} \in \mathcal{A}$,

$$M_{f_{3,i}^{(k)}\to\alpha_i^{(k)}}(\alpha) = \sum_{a'\in\mathcal{A}}\sum_{a\in\mathcal{A}} I_i(\alpha,a,a'), \tag{8}$$

where $I_i(\alpha,a,a')$ is given by (4), which under assumption (7) can be calculated in closed form. In this paper, we find the MAP estimate $\hat{\alpha}_{\text{MAP}}^{(k)}$ by an exhaustive search. However, we note that a more efficient solution is given by the expectation maximization (EM) algorithm.

c) Message Calculation for $M_{(\mathbf{H}_i^{(k-1)},A_i^{(k-1)})\to f_{3,i}^{(k)}}$ and Decision Making: Noting that the *a posteriori* probability for a transition from $A_i^{(k-1)} = a'$ to $A_i^{(k)} = a$ given α equals $I_i(\alpha,a,a')/M_{(\mathbf{H}_i^{(k-1)},A_i^{(k-1)})\to f_{3,i}^{(k)}}(\alpha)$, we calculate the Gaussian approximation of the densities $M_{(\mathbf{H}_i^{(k-1)},A_i^{(k-1)})\to f_{3,i}^{(k)}}(\mathbf{h},a)$ in (8) given the estimate $\hat{\alpha}_{\text{MAP}}^{(k)}$ as follows: Given a, we select the transition from $A_i^{(k-1)} = a'$ to $A_i^{(k)} = a$ that maximizes the *a posteriori* transition probability. If $a' = a$ maximizes the transition probability, the mean vector and the covariance matrix in (7) for the given hypothesis of a can be obtained recursively similar to the update equations of the Kalman filter, and the case $a \neq a'$ is equivalent to a re-initialization of the Kalman filter with the current channel observation. Finally, for the *a posteriori* attack probability $c_i^{(k)}$ we have

$$\begin{aligned} c_i^{(k)} = {} & I_i(\hat{\alpha}_{\text{MAP}}^{(k)},\text{Eve},D_i)/M_{(\mathbf{H}_i^{(k-1)},A_i^{(k-1)})\to f_{3,i}^{(k)}}(\hat{\alpha}_{\text{MAP}}^{(k)}) \\ & + I_i(\hat{\alpha}_{\text{MAP}}^{(k)},\text{Eve},\text{Eve})/M_{(\mathbf{H}_i^{(k-1)},A_i^{(k-1)})\to f_{3,i}^{(k)}}(\hat{\alpha}_{\text{MAP}}^{(k)}), \end{aligned}$$

and we employ the MAP decision rule for attack detection.

D. Protocol Aspects

The detection performance of our approach will strongly be affected by the correlation coefficient $\alpha_i^{(k)}$, which is determined by the frame duration T_f (or more precisely by the duration in time that lies between two transmissions of the same user) and the Doppler spectrum. To guarantee a good performance, the wireless access protocol has to ensure that the correlation coefficients are large. This can be achieved by forcing all devices to transmit at least once per frame and by enforcing transmission of pilot sequences in cases where devices do not have data to transmit. We note that this approach is also used in low-latency wireless access protocols to keep the channel knowledge up to date in order to provide devices with a guaranteed channel access (see, e.g., [6]).

E. Extensions

The framework introduced in this paper can be extended in different ways: Since common receiver architectures are based on message-passing algorithms, a natural step would be to connect the factor graph in Fig. 1 to the graph that underlies the receiver, and to utilize additional features and channel parameters. This approach would allow the AP to detect an attack already before the received packet has been completely decoded. If data models for bad-data detection are

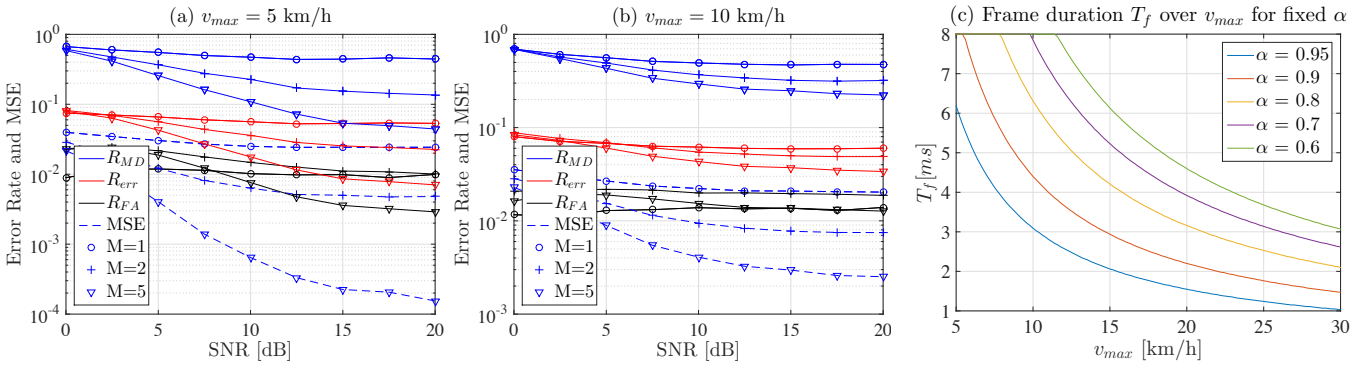

Fig. 2: Missed-detection rate R_{MD}, false-alarm rate R_{FA}, and error rate R_{err} over SNR for $v_{\max} = 5$ km/h and $v_{\max} = 10$ km/h in (a) and (b), resp., and trade-off between T_f and $v_{\max}$ for fixed correlation coefficient α.

also available, the approach presented here can be extended to enable cross-layer intrusion detection. Finally, if decision delays are permitted, the message schedule can be extended and new information can be provided to previous frames in order to update previous attack probabilities.

IV. Numerical Results

The performance of the proposed scheme is numerically evaluated through simulations of our system model for $N_c = 16$ subcarriers, channel impulse responses with $L_h = 5$ taps, the carrier frequency $f_c = 2.5$ GHz, a bandwidth of 10 MHz, and a frame period $T_f = 6$ ms. The coherence bandwidth is set to 0.1 GHz. The impact of the number of users on the performance is evaluated for $M \in \{1, 2, 5\}$ considering both a slowly changing environment with $v_{\max} = 5$ km/h and a moderately changing environment with $v_{\max} = 10$ km/h. As performance measures we study the false-alarm rate R_{FA}, the missed-detection rate R_{MD}, and the error rate R_{err} in the SNR range 0-20 dB. Since the detection performance is closely related to the accuracy of the estimate of the correlation coefficient $\alpha^{(k)}$, we also include the mean squared error $MSE = \text{E}\{(\alpha^{(k)} - \alpha_{\text{MAP}}^{(k)})^2\}$. The results are shown in Fig. 2.

In both scenarios we can see that the detection performance is improved with an increasing number of users M. For the slowly varying scenario in Fig. 2(a) the missed detection rate for $M = 5$ is reduced by one order of magnitude compared to the single-user case thanks to the high correlation with $\alpha^{(k)} \sim \text{Unif}([0.95, 1])$ for the parameter choice in this scenario. For the moderately varying scenario in Fig. 2(b), the correlation is significantly lower, $\alpha^{(k)} \sim \text{Unif}([0.81, 1])$. Still, we can observe an improved performance with an increasing number of users M; however, the gains are smaller compared to the previous case and diminish for faster scenarios under this model (e.g., $v_{\max} = 20$ km/h). A comparison of the error rates with the MSE in Fig. 2(a) and (b) reveals the importance of the accuracy of the estimate of the correlation coefficient. As soon as the MSE reaches its minimum, the error rate curves show a distinct error floor, which suggests that further performance improvements can be expected if also the temporal correlation of the correlation coefficients is utilized. In our experiments, we observed two factors that limit the accuracy of the estimate $\alpha_{\text{MAP}}^{(k)}$: For small M and low $\alpha^{(k)}$, the process noise limits the performance, whereas for large M and high $\alpha^{(k)}$, the accuracy of the sampling of the messages $M_{f_{3,i}^{(k)} \to \alpha_i^{(k)}}(\alpha)$ becomes an issue.

Finally, in order to extend the results of this paper to other parameter settings, we show in Fig. 2(c) the tradeoff between the frame duration T_f and the maximum speed $v_{\max}$ for a fixed correlation coefficient α derived from Jake's Doppler spectrum. For example, to guarantee the good performance shown in Fig. 2(a) at a maximum speed $v_{\max} = 15$ km/h, the frame duration has to be reduced to $T_f = 2$ ms, and similarly, to $T_f = 1$ ms for $v_{\max} = 30$ km/h.

V. Conclusion

We have studied a multi-user up-link scenario where an attacker tries to impersonate the legitimate transmitters. We have presented a factor-graph approach for deriving *a posteriori* attack probabilities from channel observations at the access point, which allows us to exploit the cross-channel correlation of slowly changing large-scale fading parameters for intrusion detection. As the numerical results have shown, a significantly improved detection performance is obtained in channels with high correlation. The gain is primarily due to the improved accuracy of the parameter estimation. Since our approach can be integrated into state-of-the-art iterative receiver architectures, it enables joint decoding and intrusion detection and is well suited for low-latency applications.

References

[1] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 56–62, October 2010.

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

[3] P. Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over MIMO fading wiretap channels," *IEEE Trans. on Wireless Communications*, vol. 11, no. 7, pp. 2564–2573, Jul. 2012.

[4] S. Van Vaerenbergh, Ó González, J. Via, and I. Santamara, "Physical layer authentication based on channel response tracking using Gaussian processes," in *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, May 2014, pp. 2410–2414.

[5] F.R. Kschischang, B.J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 498–519, 2001.

[6] C. Dombrowski and J. Gross, "EchoRing: A low-latency, reliable token-passing MAC protocol for wireless industrial networks," in *Proc. European Wireless Conference 2015*. VDE, 2015, pp. 1–8.