An Information Theoretic Approach to RF Fingerprinting

Onur Gungor, C. Emre Koksal, Hesham El Gamal

***Abstract*—RF fingerprinting exploits the variations in the RF chain of radios to uniquely identify transmitters, and distinguish adversarial transmissions from legitimate nodes. We provide a systematic approach rooted from information theory to understand basic performance limits of RF fingerprinting. We develop a novel channel model to cover RF fingerprinting systems, where the imperfections in the RF chain are modeled as a *fingerprint channel*, cascaded to the physical channel. We analyze authentication problem in the presence of an adversary, where both the legitimate transmitter and the adversary are equipped with unique fingerprint channels. We provide bounds for the error exponents of the legitimate nodes, and the success exponent of the adversary, as a function of their fingerprints. We illustrate that concepts analogous to Maurer's simulatability are necessary to guarantee authentication via RF fingerprints.**

I. Introduction

Authentication is the act of confirming the identity of a device, person, or software. Authentication between two devices can be achieved by exploiting various sources of common randomness that cannot be reproduced by an adversary. In computer science, authentication is generally performed by utilizing *secret key bits*, that are assumed to be available exclusively to the legitimate nodes [1]. However, this assumption may be too restrictive in general. Recent works have sought other sources of common randomness for authentication. For instance, wireless channel based authentication [2] exploits the characteristics of multipath fading to authenticate a transmitter. Another recently proposed method is to exploit the *RF Fingerprints* of the transmitters. It has been shown that even different radios of the same make and brand preserve different characteristics, due to unique imperfections in digital-analog converters and power amplifiers [3].

Various algorithms have been proposed in the literature to exploit the RF Fingerprints for authentication. These approaches can be considered in two categories; transient based implementations [3]–[5] perform classification based on the amplitude/phase characterization of the signal envelope, and modulation based implementations [6] perform classification based on frequency offset, sync correlation, etc. However, as far as we are aware of, a fundamental approach is missing, which is required to provide answers to the questions: i) When is authentication possible? ii) What is the probability of authentication error for the best scheme?

O. Gungor, C. E. Koksal and H. El Gamal are with the Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH, 43210 (e-mail: gungoro@ece.osu.edu, koksal@ece.osu.edu, helgamal@ece.osu.edu).

This publication was made possible by NPRP grant #5-559-2-227 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

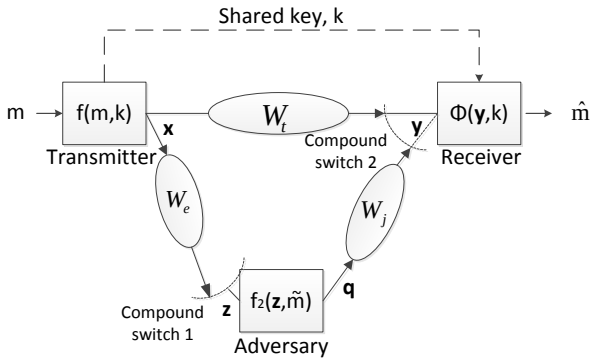

Fig. 1. System Model

In order to provide answers to these questions, we consider an information theoretic approach to RF-fingerprinting, in a point-to-point authentication framework in the presence of an active adversary, shown in Figure 1. To observe the effects of RF-fingerprints on authentication, we model the RF-fingerprints as a channel cascaded to the physical channel, as shown in Figure 2. We find theoretical bounds on the error and attack probability exponents, and illustrate that there is a trade-off between probabilities of success under an attack, and error under no attack. Our strategy involves the use of errors-and-erasures decoder as used in [7]. We illustrate that, when there is no shared secret key between the legitimate nodes, the capacity is 0 if the legitimate channel is simulatable by the adversary, a condition which is similar to the condition introduced by Maurer for the source model [8]. Otherwise, the capacity is equal to the capacity of the channel without any adversary. In other words, it is not possible to avoid attacks without unique RF-fingerprints that satisfy non-simulatability condition. We find necessary conditions for RF-fingerprint channels to ensure non-simulatability, Finally, we provide a graphical approach to confirm whether the adversary can simulate W_t.

A. Related Work

i) *Authentication* problem was first studied from a theoretical point of view by Simmons [9] for a special case of Figure 1, where all of the channels are noiseless (i.e., without any RF-fingerprints). His analysis, which relied on secret key based authentication, has been extended to different

settings over the years, see e.g. [10], [11]. To the best of our knowledge, none of the extensions included RF-fingerprints.
ii) *Arbitrarily Varying Channels* model memoryless channels whose law vary in an arbitrary and unknown manner to the legitimate nodes, possibly under the influence of an adversary [12]. This channel is especially more suitable to model substitution attacks in a wireless setting, where the equivalent channel is a function of both the transmitter and adversary signal. However, the works in the literature only focus on reliable communication, i.e., we have not come across any work that studies arbitrarily varying channels in authentication framework.
iii) *Watermarking* studies the problem of hiding a message into a covertext signal under a distortion constraint [13]. For instance, Alice, who shares a key with Bob, hides a message to a music file in such a way the music file is still playable (not significantly distorted), and the message is recoverable only by Bob. Eve, not having access to this key, distorts the message in an arbitrary manner to make the message unrecoverable by Bob. Although the tools used are similar, this problem has not been studied under the context of RF fingerprinting.

II. System Model

We consider the model depicted in Figure 1. Random variables are denoted by capital letters, whereas their realizations are denoted by lower case letters, and random vectors of size n are denoted by boldface letters. $\mathbf{X} = [X_1, \ldots, X_n]$ is the signal transmitted by the legitimate transmitter over n channel uses, whereas $\mathbf{Z}$, $\mathbf{Q}$ and $\mathbf{Y}$ denote the received signal by the adversary, the modified signal at the adversary encoder, and the received signal by the legitimate receiver, respectively. Calligraphic letters are used to denote (finite size) alphabets. We will use the notation in [14] to represent types. A vector $\mathbf{x}$ is of type P, if $\frac{1}{n}\Pi(a|\mathbf{x}) = P(a),\ \forall a \in \mathcal{X}$, where $\Pi(a|\mathbf{x})$ denotes the number of occurrences of a in the vector $\mathbf{x}$. We denote the type class P by $\mathcal{T}_P$. Similarly, we define the conditional type class $\mathcal{T}_V(\mathbf{x})$ by the set of vectors $\mathbf{y}$ which satisfies the condition

$$\Pi(a, b|\mathbf{x}, \mathbf{y}) = P(a)V(b|a),\ \forall a, b.$$

We will interchangeably use the notations $H(P) \equiv H(X)$ to denote the entropy of a random variable X with distribution P, and $I(P, V) \equiv I(X; Y)$ to denote the mutual information between X and Y, whose conditional probability distribution based on X is V. Information divergence between two conditional distributions V and W conditioned on P is defined as

$$\begin{aligned} D(V\|W|P) &\triangleq \sum_{a\in\mathcal{X}} P(a) D(V(.|a)\|W(.|a)) \\ &= \sum_{a\in\mathcal{X}}\sum_{c\in\mathcal{Y}} P(a)V(c|a)\log\left(\frac{V(c|a)}{W(c|a)}\right) \end{aligned}$$

A. RF Fingerprints

We incorporate the RF fingerprints into our model in Figure 1 as follows. The RF fingerprint of the transmitter and the adversary are denoted as *RF fingerprint channels* $W_{t,f}$ and $W_{j,f}$, respectively, which models the imperfections from the encoder output to the transmitting antenna. Let us the denote *physical channels*[1] between transmitter to receiver, transmitter to adversary, and adversary to receiver as $W_{t,c}$, $W_{e,c}$ and $W_{j,c}$, respectively. Therefore, the equivalent channels are formed via a cascade of RF fingerprint channels and physical channels, as shown in Figure 2. Therefore, the equivalent channels can be written as

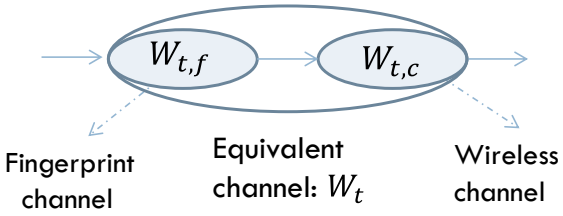

Fig. 2. Equivalent channel is a cascade of RF fingerprint channel and physical channel.

$$\begin{aligned} W_t &\triangleq W_{t,f} * W_{t,c} \\ W_e &\triangleq W_{t,f} * W_{e,c} \\ W_j &\triangleq W_{j,f} * W_{j,c} \end{aligned}$$

where $*$ is the convolution operator, i.e.,

$$(W_{t,f} * W_{t,c})(c|a) = \sum_b W_{t,f}(b|a)W_{t,c}(c|b), \forall\ a, c \qquad (1)$$

B. Attack Model

The legitimate transmitter attempts to send a message $m \in \{1, \ldots, 2^{nR}\}$ to the legitimate receiver, in the presence of the adversary. They are assumed to share a key $k \in \{1, \ldots, 2^{nR_K}\}$ beforehand. The transmitter encodes the message m to $\mathbf{x} = f(m, k)$ via a mapping f, and transmits $\mathbf{x}$ over the channel. The receiver obtains signal $\mathbf{y}$, and extracts $\hat{m} = \phi(\mathbf{y}, k) \in \{0, 1, \ldots, 2^{nR}\}$ via a decoding function ϕ, where 0 corresponds to an erasure. The received signal $\mathbf{y}$ depends on the positions of the compound switches in Figure 1. There are three different modes of operation:

1) *No attack*: Switch 2 is closed on the main channel W_t.
2) *Impersonation attack*: Switch 1 is open, yet switch 2 is closed on the jammer channel W_j. Let the adversary attempt to make the receiver decode $\tilde{m}$. Then, the adversary transmits a signal $\mathbf{q}$, independent of the transmitter's signal $\mathbf{x}$, through an arbitrary mapping $\mathbf{q} = f_2(\tilde{m})$, which after passing through W_j, yields $\mathbf{y}$.
3) *Substitution attack*: In contrast with the impersonation attack, switch 1 is also closed. The adversary intercepts $\mathbf{x} = f(m, k)$ through the channel W_e and receives $\mathbf{z}$. To make the receiver decode $\tilde{m}$, the adversary encodes $\mathbf{q} = f_2(\tilde{m}, \mathbf{z})$ via an arbitrary mapping f_2 (which can

[1]The channel between the transmitting antenna and the receiving antenna.

be random), and transmits $\mathbf{q}$ over the channel W_j, which yields $\mathbf{y}$.

We define the error events for these three cases. For no attack, we define the following events, conditioned on the fact that $\mathbf{x} = f(m,k)$ is transmitted

$$\begin{aligned} &s_{na}|m,k:\phi(\mathbf{y},k)=m \\ &\alpha_{na}|m,k:\phi(\mathbf{y},k)=0 \\ &\varepsilon_{na}|m,k:\phi(\mathbf{y},k)=m',\ \exists m'\neq m,\ m'\neq 0 \end{aligned}$$

where s_{na}, α_{na} and ε_{na} denote success, erasure and (undetected) error events, respectively. For impersonation attack, we similarly define the events, conditioned on the fact that key is k, and adversary transmits $\mathbf{q} = f_2(\tilde{m})$

$$\begin{aligned} &s_{imp}|\tilde{m},k:\phi(\mathbf{y},k)=\tilde{m} \\ &\alpha_{imp}|\tilde{m},k:\phi(\mathbf{y},k)=0 \\ &\varepsilon_{imp}|\tilde{m},k:\phi(\mathbf{y},k)=m',\ \exists m'\neq \tilde{m},\ m'\neq 0 \end{aligned}$$

Finally, for substitution attack, events are based on the fact that $\mathbf{x} = f(m,k)$ is intercepted by the adversary, who transmits $\mathbf{q} = f_2(\tilde{m},\mathbf{z})$

$$\begin{aligned} &s_{sub}|m,\tilde{m},k:\phi(\mathbf{y},k)=\tilde{m} \\ &\alpha_{sub}|m,\tilde{m},k:\phi(\mathbf{y},k)=0 \\ &\varepsilon_{sub}|m,\tilde{m},k:\phi(\mathbf{y},k)=m',\ \exists m'\neq \tilde{m},\ m'\neq 0 \end{aligned}$$

Definition 1. *When a key stream of rate R_K is available to the legitimate nodes prior to communication, rate $R(R_K)$ is achievable robustly if for any $\epsilon > 0$, there exists a block length n large enough, and a coding scheme (f,ϕ) such that*

$$\mathbb{P}(\alpha_{na} \cup \varepsilon_{na}|m,k) \leq \epsilon \tag{2}$$
$$\mathbb{P}(s_{imp} \cup \varepsilon_{imp}|\tilde{m},k) \leq \epsilon \tag{3}$$
$$\mathbb{P}(s_{sub} \cup \varepsilon_{sub}|m,\tilde{m},k) \leq \epsilon \tag{4}$$

for any $m,\tilde{m},k$, under any possible adversary attack strategy f_2.

Authentication capacity $C(R_K)$ is the supremum of robust achievable rates[2]. We are both interested in the authentication capacity, and the exponential rate of decay of the probability expressions in (2)-(4). We will use capital letters to refer to these exponents, e.g., for no attack $S_{na} = -\frac{1}{n}\log\mathbb{P}(s_{na})$, $A_{na} = -\frac{1}{n}\log\mathbb{P}(\alpha_{na})$, and $E_{na} = -\frac{1}{n}\log\mathbb{P}(\varepsilon_{na})$. We will also use the notation

$$E_{sp}(R,P,W) \triangleq \min_{V:I(P,V)\leq R} D(V\|W|P) \tag{5}$$

to refer to the sphere packing exponent [14]; the maximum error exponent achievable via any constant composition codebook. We will also use the inverse sphere packing function

$$E_{sp}^{-1}(x,P,W) \triangleq \inf\{R : E_{sp}(R,P,W) \leq x\} \tag{6}$$

[2]One may also consider a weaker definition, where the probabilities of undetected error events under impersonation and substitution attacks (3),(4) are not bounded.

C. Assumptions

In this work, we restrict ourselves to the case where all (RF fingerprint and physical) channels to be discrete memoryless channels (DMC) [3]. Although our model system model is provided in the most general form, our results are limited to the case where there is no common key ($K = \emptyset$) between the legitimate nodes. We assume that the receiver perfectly knows the equivalent transmitter channel (W_t), yet it has no information about the other channels (i.e., W_j, W_e). Finally, note that we assumed there is a compound switch that is controlled by an adversary, i.e., when no attack occurs, the equivalent channel the receiver observes is W_t, which is independent of jammer channel, and when attack occurs, the receiver observes W_j, which is independent of transmitter channel. For substitution attacks, the model may not be sufficient to represent wireless channels, which are prone to interference. To analyze substitution attacks in a wireless setting, modeling the equivalent channel as an arbitrarily varying channel may be more suitable (see Section I-A).

III. Main Results

We assume there is no common key shared between the legitimate nodes, i.e., $R_K = 0$. Listening to the legitimate transmitter's signal would provide no benefit to the adversary, hence substitution attack probabilities cannot be higher than impersonation attack probabilities. Therefore, we only analyze impersonation attacks.

Let $Q : \mathcal{X} \to \mathcal{Q}$ denote a transition probability function, and define $W_{jQ} \triangleq Q * W_j$, i.e.,

$$W_{jQ}(c|a) = \sum_c Q(b|a)W_j(c|b),\ \forall a,c \tag{7}$$

Definition 2. *The adversary can* simulate *the legitimate channel if there is some W_{jQ} such that*

$$W_{jQ}(c|a) = W_t(c|a),\ \forall a,c$$

Now, we show that positive exponential decay of probabilities of events α_{na}, ε_{na}, s_{imp} and ε_{imp} can be attained if the adversary cannot simulate the legitimate channel. Our scheme is based on using a constant composition encoder, and an errors-erasures decoder [7] that is tuned to the legitimate channel W_t.

Theorem 1. *Let $R_K = 0$, and*

$$\min_Q \max_{a\in\mathcal{X}} \sum_{c\in\mathcal{Y}} |W_{jQ}(c|a) - W_t(c|a)| \geq \eta \tag{8}$$

Let $\xi > 0$ be a constant and P be a type in $\mathcal{X}$. Let $P(a^*) = \max_{a\in\mathcal{X}} P(a)$. Then, the exponents

$$A_{na} \geq \xi \tag{9}$$
$$E_{na} \geq \min_{0\leq\xi'\leq\xi} E_{sp}(R+\xi-\xi',P,W_t) + |E_{sp}^{-1}(\xi',P,W_t) - R|^+ \tag{10}$$

[3]In reality, the channels are neither discrete, nor memoryless. We incorporated these assumptions to simplify our analysis. Extending our analysis to continuous channels with memory is part of our future work.

$$S_{imp} \geq \frac{1}{2}P(a^*)\left[\eta - \sqrt{\frac{2\xi}{P(a^*)}}\right]^2 \tag{11}$$

$$E_{imp} \geq \min_{Q} \min_{0\leq\xi'\leq\xi} E_{sp}(R+\xi-\xi', P, W_{jQ}) + |E_{sp}^{-1}(\xi', P, W_t) - R|^+ \tag{12}$$

are simultaneously achievable.

The proof is omitted due to space constraints. Note that the exponents under no attack S_{na} and E_{na} also appear in [7]. Before we further analyze the exponents, we provide a lemma on the properties of the sphere packing exponent, E_{sp}.

Lemma 1. *There exists $R_{\inf} > 0$, such that the sphere packing exponent $E_{sp}(R, P, W)$ is a convex and strictly decreasing function of R in the interval $[R_{\inf}, I(P, W)]$, and*

$$E_{sp}(R, P, W) = \min_{V: I(P,V)=R} D(V\|W|P)$$

For the proof of this lemma, see Lemma 10.4 of [14]. Based on this, we can see that there exists $R^* > 0$ such that, $\frac{\partial E_{sp}(R,P,W)}{\partial R} > -1$ for $R \geq R^*$, which we refer to as the *critical point*. Let $\xi^* = E_{sp}(R^*, P, W)$. Then, $E_{sp}^{-1}(\xi, P, W)$ is also a convex and strictly decreasing function of τ, and we can see that $\frac{\partial E_{sp}^{-1}(\xi,P,W)}{\partial \xi} < -1$ for $\xi < \xi^*$. Let R_t^* and R_{jQ}^* be the critical points of functions $E_{sp}(R, P, W_t)$ and $E_{sp}(R, P, W_{jQ})$, respectively, and similarly define ξ_t^* and ξ_{jQ}^*.

Corollary 1. *For ξ and R such that $\max(R_t^*, R_{jQ}^*) < R \leq I(P, W_t)$, and $E_{sp}(R, P, W_t) < \xi$,*

$$E_{na} \geq E_{sp}(R, P, W_t) + E_{sp}^{-1}(\xi, P, W_t) - R > 0 \tag{13}$$

$$E_{imp} \geq E_{sp}(R, P, W_{jQ}) + E_{sp}^{-1}(\xi, P, W_t) - R > 0 \tag{14}$$

Proof: For both terms, the first inequality follows since in (10) and (12), the minima is attained at $\xi' = \xi$. Since $E_{sp}(R, P, W_t)$ is strictly decreasing, and $E_{sp}(R, P, W_t) < \xi$, therefore $E_{sp}^{-1}(\xi, P, W_t) > R$, which indicates that both terms are positive. ∎

Theorem 2. *Let $R_K = 0$. If the adversary cannot* simulate *the legitimate channel, $C = \max_P I(P, W_t)$, i.e., authentication capacity is equal to the Shannon capacity. Otherwise, $C = 0$.*

Proof: The proof follows from Theorem 1 and Corollary 1. When the adversary cannot simulate the legitimate channel, η, as defined in (8) is positive. Fix a type P. Let $\delta > 0$ be small enough such that $R = I(P, W_t) - \delta \geq \max(R_t^*, R_{jQ}^*)$. Let $\xi > 0$ be small enough such that $\eta - \sqrt{\frac{2\xi}{P(a^*)}}$, and $E_{sp}^{-1}(\xi, P, W_t) > R$. Then, according to Corollary 1, $E_{na} > 0$ and $E_{imp} > 0$. Furthermore, due positivity of η, and the choice of ξ, $A_{na} > 0$ and $S_{imp} > 0$, which concludes that rate R is achievable. The converse follows since when $\eta = 0$, both channels are identical. When $W_{jQ}(c|a) = W_t(c|a)$ for any a, c, for any coding scheme (f, ϕ) such that $\mathbb{P}(s_{na}) \geq 1 - \epsilon$, it can be seen that $\mathbb{P}(s_{imp}) \geq 1 - \epsilon$ as well. ∎

IV. Numerical Evaluation

In this section, we illustrate our findings in a numerical example. We consider all channels to be ternary, and choose

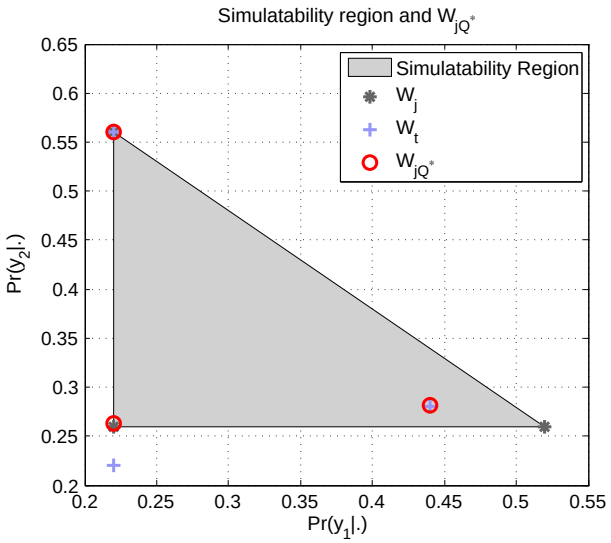

Fig. 3. Simulatability Region

the transition probability functions (in matrix form) as

$$W_{t,f} = \begin{pmatrix} 0.6 & 0.2 & 0.2 \\ 0.05 & 0.9 & 0.05 \\ 0.05 & 0.5 & 0.9 \end{pmatrix}, W_{j,f} = \begin{pmatrix} 0.8 & 0.15 & 0.05 \\ 0.05 & 0.9 & 0.05 \\ 0.05 & 0.15 & 0.8 \end{pmatrix}$$

$$W_{t,c} = W_{j,c} = \begin{pmatrix} 0.6 & 0.2 & 0.2 \\ 0.2 & 0.6 & 0.2 \\ 0.2 & 0.2 & 0.6 \end{pmatrix}$$

We can obtain the equivalent channels in matrix form as

$$W_t = \begin{pmatrix} 0.44 & 0.28 & 0.28 \\ 0.22 & 0.56 & 0.22 \\ 0.22 & 0.22 & 0.56 \end{pmatrix}, W_j = \begin{pmatrix} 0.52 & 0.26 & 0.22 \\ 0.22 & 0.56 & 0.22 \\ 0.22 & 0.26 & 0.52 \end{pmatrix}$$

where $W_t = W_{t,f}W_{t,c}$, and $W_j = W_{j,f}W_{j,c}$. Now, we provide a graphical approach that shows whether W_t is simulatable. Note that, the transition probability matrices can be uniquely determined from the first $|\mathcal{Y}| - 1 = 2$ indices, which are plotted in Figure 3. Via a prefix channel Q, the adversary can achieve any point inside the triangle that points of W_j form by achieving the equivalent channel $W_{jQ} = Q * W_j$, as in (7). The convex hull of points of W_j is called the *simulatability region*. If any point of W_t falls outside the simulatability region, then W_t is not simulatable, which is indeed the case for our numerical example. Furthermore, parameter η in (8) is equal to the maximum of the $L-1$ distances from the points of W_t to the simulatability region, which is equal to $\eta = 0.0453$ in our example. Since W_t is not simulatable, the capacity is equal to Shannon capacity by Theorem 2, which is found to be $C = 0.12$ bits /chn use.

For this example, we also evaluate the error/success exponents in Theorem 1. In Figure 4, we plot the exponents as a function of coding rate R, where we fixed the erasure parameter to be $\xi = \xi_{\max}/2$, and in Figure 5, we plot the exponents as a function of erasure parameter ξ, where we fixed the coding rate $R = 0.8C$. Notice that the trade-off between the impersonation attack success probability and the erasure probability under no attack, is clearly visible.

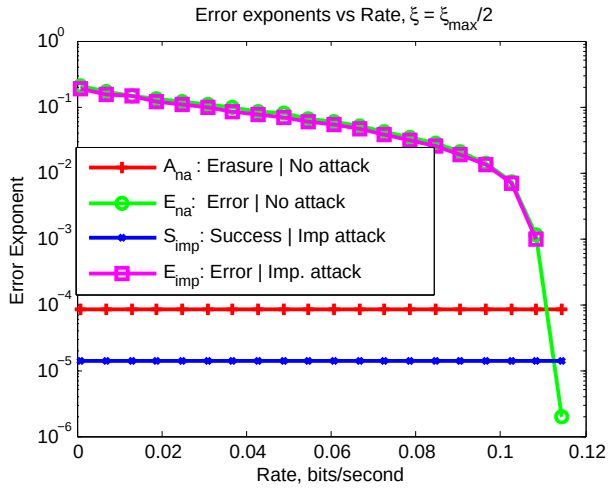

Fig. 4. Error/Success exponents as a function of rate R

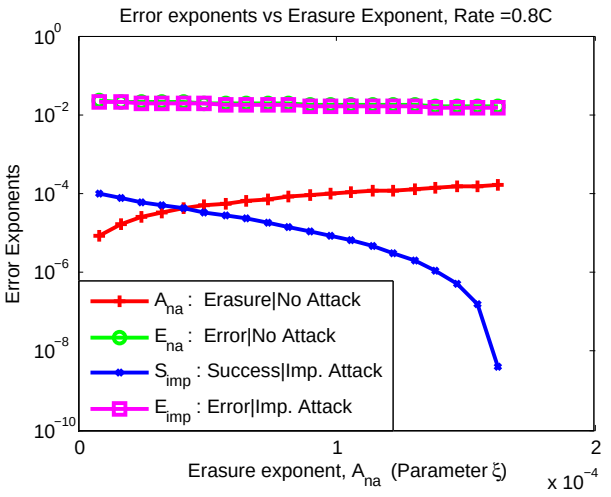

Fig. 5. Error/Success exponents as a function of erasure exponent, $A_{na} = \xi$

V. Conclusions

In this work, we introduced a model to analyze the performance of RF-fingerprinting in authentication framework. We modeled the imperfections of the transmitters as fingerprint channels that are cascaded to the physical channels. We evaluated the error and success exponents, and illustrated the tradeoff between erasure probability under no attack, and success probability under impersonation attack. We also showed that, if the adversary can simulate the legitimate channel, then authentication is not possible. Otherwise, rates up to Shannon capacity can be achieved. Our future investigations include i) obtaining complete characterization of error exponents when there are shared secret keys between the legitimate nodes, by combining Lai's approach with ours, ii) considering more realistic settings where the channels are not memoryless, and continuous, and the main channel is not perfectly known at the transmitter.

References

[1] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, "Umac: Fast and secure message authentication," in *Advances in Cryptology-CRYPTO99*, pp. 216–233, Springer, 1999.

[2] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *Communications, 2007. ICC'07. IEEE International Conference on*, pp. 4646–4651, IEEE, 2007.

[3] O. Ureten and N. Serinken, "Wireless security through rf fingerprinting," *Electrical and Computer Engineering, Canadian Journal of*, vol. 32, no. 1, pp. 27–33, 2007.

[4] B. Danev, T. S. Heydt-Benjamin, and S. Capkun, "Physical-layer identification of rfid devices.," in *Usenix Security Symposium*, pp. 199–214, 2009.

[5] B. Danev and S. Capkun, "Transient-based identification of wireless sensor nodes," in *Proceedings of the 2009 International Conference on Information Processing in Sensor Networks*, pp. 25–36, IEEE Computer Society, 2009.

[6] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pp. 116–127, ACM, 2008.

[7] I. E. Telatar *et al.*, *Multi-access communications with decision feedback decoding*. PhD thesis, Massachusetts Institute of Technology, 1992.

[8] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels-part ii: the simulatability condition," *Information Theory, IEEE Transactions on*, vol. 49, no. 4, pp. 832–838, 2003.

[9] G. J. Simmons, "Authentication theory/coding theory," in *Advances in Cryptology*, pp. 411–431, Springer, 1985.

[10] U. M. Maurer, "Authentication theory and hypothesis testing," *Information Theory, IEEE Transactions on*, vol. 46, no. 4, pp. 1350–1356, 2000.

[11] L. Lai, H. El Gamal, and H. V. Poor, "Authentication over noisy channels," *Information Theory, IEEE Transactions on*, vol. 55, no. 2, pp. 906–916, 2009.

[12] A. Lapidoth and P. Narayan, "Reliable communication under channel uncertainty," *Information Theory, IEEE Transactions on*, vol. 44, no. 6, pp. 2148–2177, 1998.

[13] A. Somekh-Baruch and N. Merhav, "On the error exponent and capacity games of private watermarking systems," *Information Theory, IEEE Transactions on*, vol. 49, no. 3, pp. 537–562, 2003.

[14] I. Csiszar and J. Körner, *Information theory: coding theorems for discrete memoryless systems*. Cambridge University Press, 2011.