Challenge-Response Physical Layer Authentication Over Partially Controllable Channels

Stefano Tomasin, Hongliang Zhang, Arsenia Chorti, and H. Vincent Poor

***Abstract*—Challenge-response is a security mechanism well known for authentication using encryption. In this paper, we propose new challenge-response mechanisms in the context of physical layer security (PLS). The verifier, instead of sending a challenge, changes the physical properties of the electromagnetic environment and expects to receive a properly modified signal from the device under verification. We thus introduce the concept of *partially controllable channels* that enable such signal propagation medium changes. We also show that current and future communication systems already entail several examples of such partially controllable channels, e.g., when using intelligent reflective surfaces (IRSs) or relays, or for communications among drones. Several security issues associated with the new challenge-response mechanisms are discussed and future topics to be investigated are outlined.**

INTRODUCTION

Message authentication mechanisms enable an agent (Bob) to confirm that a received message has been transmitted by another specific agent (Alice), rather than by a malicious agent (Eve), who, in turn, aims at impersonating Alice. Two main classes of such mechanisms are tag-based (TB) and challenge-response (CR) authentication. With the TB authentication mechanism, the message incorporates a tag or identifier that can only be generated by Alice and recognized by Bob: for example, Alice and Bob share a secret key, by which Alice encodes an information related to the message (e.g., its checksum and timestamp) that is then decoded and verified by Bob to confirm that Alice was the sender. With the CR authentication mechanism, instead, Alice and Bob share a secret that enables Bob to ask random questions to Alice, who is the only one able to provide the correct answer. In everyday life, signing a letter is a TB authentication mechanism, while using a one-time password (OTP) is a CR authentication mechanism.

Both TB and CR authentication mechanisms among machines are typically implemented with encryption schemes. TB authentication can be achieved by encrypting the message with the private key of an asymmetric key encryption system. With a CR solution, instead, Alice applies a pre-determined function (known to Bob) to the challenge and encrypts it with a symmetric key (known only to Bob) before transmission.

Recently, alternative or complementary mechanisms to security without using encryption have been investigated: they can be suitable for devices with limited capabilities or in scenarios with light infrastructures, e.g., without trusted servers or key distribution protocols. Here, we focus on physical-layer security (PLS) [1], a branch of information security that studies mechanisms leveraging the properties of the physical channel over which transmissions occur.

Authentication mechanisms have been studied also in PLS (see [2] for a recent survey), and in particular TB authentication has been mostly studied, using as tag the channel state information (CSI), e.g., the gain, impulse, or frequency response of the channel. In turn, CR authentication in PLS has been scarcely studied until now. In [3], a CR PLS mechanism is proposed: the channel is used to hide both the challenge and the response from Eve using a PLS confidentiality mechanism, preventing her from generating the correct response. This approach has been extended in [4] by adding artificial noise to further protect the shared secret. A similar concept has been introduced in [5], where a set of sensors is protected against impersonation by using a set of actuators that continually challenge the surrounding environment via random but deliberate physical probes that are then detected by the sensors. Also in this case, the challenge comes from the actuator, and the timing of the challenge is relevant. Lastly, in [6] a CR mechanism is proposed, wherein the verifier asks the node under control to report the CSI of a selected frequency, different from that on which the message is transmitted.

In this paper, we introduce a new mechanism for CR PLS authentication to be applied on channels that can be (at least partially) *controlled* by Bob, i.e., whose propagation characteristics can be in part determined by Bob. In such a scenario, the challenge is represented by setting some channel parameters (*channel configuration*) that however do not completely determine the channel; the response is represented by the CSI estimated by Bob, which should be consistent with the selected configuration. By preventing Eve from knowing the current channel configuration, Eve will not be able to provide the correct response to Bob. Note that, in [4], the channel randomness determines the amount of secret information shared by Alice and Bob, while in our mechanism the size of the secret is determined by how much control Bob has on the channel. Note also that our mechanism *modifies* the channel, while in [6] a feature of an existing channel is *selected* for authentication. We also argue that this mechanism can be extended to include contextual information that is unique during communications between Alice and Bob, e.g., relative angle of arrival / departure or amplitude of received signals in a vehicle-to-vehicle scenario. Whenever the context is in part controllable by Bob, a CR PLS authentication mechanism can be designed.

Stefano Tomasin is with the University of Padova, Italy, and with the CNIT, the National Inter-University Consortium for Telecommunications, Italy.

Hongliang Zhang and H. Vincent Poor are with Princeton University, USA.

Arsenia Chorti is with ETIS UMR 8051, CYU, ENSEA, CNRS (FR) and with the Barkhausen Institut gGmbH (DE).

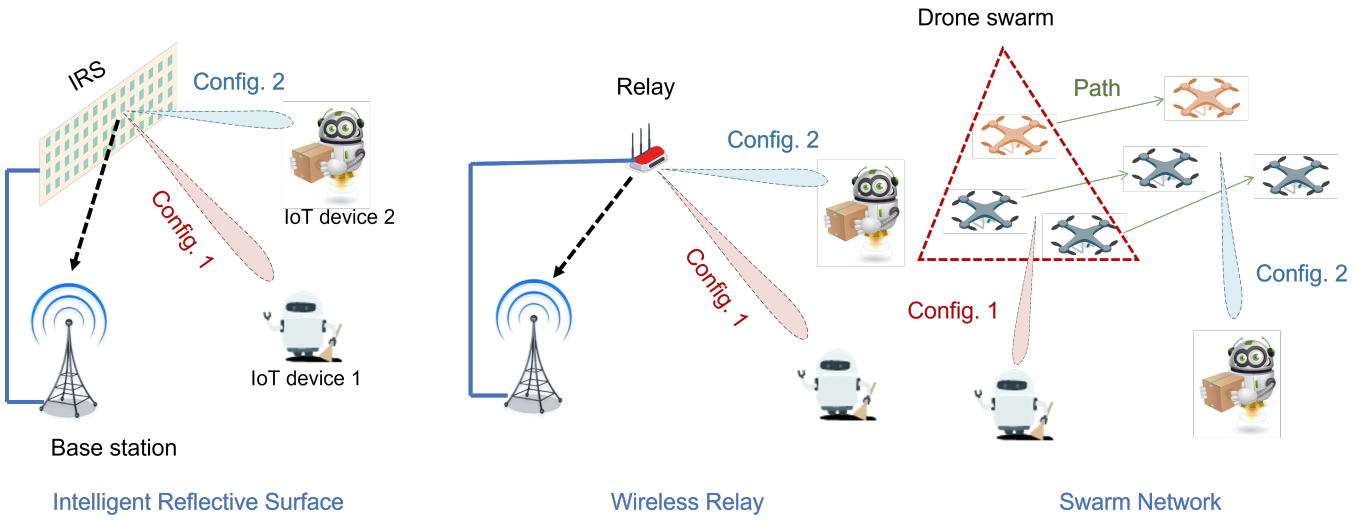

Figure 1. Three examples for partially controllable channels.

Partially Controllable Contexts

Future wireless technologies are expected to enable secure communications without relying on, e.g., long-term secure storage or central trusted parties. New opportunistic pairing protocols will turn related readings (e.g., movement, location, camera inputs, or radio measurements) into authentication parameters. Such approaches will allow devices to autonomously establish trust for peer-to-peer and group communications in demanding scenarios, e.g., car platoons, drone swarms, or industrial applications. In this paper, we focus on *contexts* that can be in part controllable, i.e., their properties can be modified by some of the agents in the network (communicating devices), see also [7]. For example, devices with light sensors or cameras may be connected to an infrastructure able to partially control the light (e.g., by controlling dimmable artificial lights). In the following, a *configuration* of the channel refers to a specific set of channel parameters that are controlled by Bob and induce a specific CSI at Bob.

As detailed in the rest of this paper, beyond partial controllability, CR PLS authentication also has other requirements: the CSI estimated by Bob should be slowly time-varying (including the effects of environmental changes), while exhibiting a high variance with the position of both the transmitter and the receiver. The first property is exploited when comparing CSI values obtained by the same device in different times, while the latter property ensures that when either Alice or Eve transmit (from different locations), Bob estimates remarkably different CSI values. Moreover, the channel must exhibit a high variance with respect to its configuration, to make it unpredictable to Eve.

We now provide examples involving intelligent reflective surfaces (IRSs), relays, and swarms, as summarized in Fig. 1.

Intelligent Reflective Surfaces: An IRS is a panel of tiled metamaterial elements that reflect impinging radio signals with controllable phases, steering them in desired directions. A particular choice of the phase values for all IRS elements provides an IRS configuration. In future cellular networks, IRSs are envisioned to be controlled by base stations, mostly with the objective of increasing coverage, especially at high frequencies (both for millimeter waves and in the THz band). For our authentication purpose, Bob is the base station, which also exclusively controls the IRS, while Alice and Eve are devices in the cell. Bob has a controllable channel available, according to the selected IRS configuration. IRSs are suitable for CR PLS authentication, as they have a high and controllable directivity, thus providing significantly different channels to different devices (Alice and Eve in our scenario). For the same reason, IRSs have been considered for achieving confidentiality using PLS techniques, and they have also been studied for performing confidentiality attacks when under the control of an eavesdropper [8]. Moreover, the large number of elements of the IRS provides a large control space and a high variance on the obtained channels.

Wireless Relays: Relays receive radio signals from specific directions by combining the signals at their multiple antennas and then re-transmit the signals in other directions with suitable transmit beamformers and amplifications. Such devices have fewer antennas than IRS elements, but have more elaborate signal processing and estimation capabilities, thus being more flexible in adapting to the electromagnetic environment. When the relay (i.e., its combiner and beamformer) is under the control of Bob, it operates as the controllable part of the channel. The relay *configuration* indicates the specific combiners and beamformers the relay uses to receive and transmit signals. Also in this case, we have the desired directivity to distinguish between Alice and Eve from the CSI estimated by Bob.

Both IRSs and relays are prominent examples of how the electromagnetic environment can be made *smart* [9], i.e., adaptive, to increase the coverage of base stations in current and future cellular networks.

Swarm Networks: The third class of controllable channels is obtained by letting multiple devices cooperate. For example, trusted drones in a swarm may cooperate with a central entity (e.g., one drone of the same group, shown in

orange in Fig. 1) for the authentication of received messages. The entire swarm is Bob, and the channel from the message source (Alice) to Bob can be partially controlled by changing the position of the drones. The large number of possible positions taken by the drones ensures a large control space and highly variable channels, as well as a spatial differentiation of the estimated CSI when Alice and Eve are transmitting. Another example is a group of vehicles (e.g., a platoon), whose positions can be controlled for the authentication of messages coming from the roadside in infrastructure-to-vehicle communications. The *channel configuration* in this scenario refers to the position of the drones or vehicles. We note in passing that in [10] a proximity estimation TB mechanism was introduced by inducing randomness through the mobility of Bob, who could make measurements from various unpredictable locations.

Four remarks are in order now:

- While we focus here on authentication, other security primitives might also benefit from channel controllability. For example, data confidentiality has also been considered in the context of the above three partially controllable channels [11]–[13].
- Other partially controllable contexts can be considered. For example, changing lighting conditions by authentication systems based on image recognition provides a partially controllable context. Still, the transmission technique described in [5] does not provide a controllable channel, but rather is a side communication channel used for security purposes.
- CR protocols can also be built by exploiting physically unclonable functions (PUFs) and combined with other PLS schemes [10]; however, the underlying principle relies on the variations of physical phenomena (e.g., temperature or vibrations) during silica fabrication, so this concept is fundamentally different from that proposed in this work.
- While exploiting channel controllability for authentication, we should also satisfy external (non security-related) constraints. For example, channel changes affect both the quality of the communication and the energy consumption (especially to move drones or vehicles). Moreover, the position of drones and vehicles in platoons typically will be subject to strict rules depending on safety and traffic.

We now focus on the authentication problem, first giving a brief overview of the existing TB PLS authentication, and then introducing the new CR PLS authentication.

Tag-Based PLS Authentication

The TB PLS authentication mechanism comprises the following steps (see also Fig. 2):

1) *Step 1 identification association*: Alice sends Bob a publicly known *pilot signal* with some other authentication mechanisms, e.g., operating at the upper communication layers. Bob estimates the CSI (e.g., the impulse or frequency response, or the received signal power, or the channel duration) using the pilot signal and stores it as the *identifier* of Alice. This step occurs only once, or anytime the channel changes significantly.
2) *Step 2 identification verification*: Bob receives a message and seeks to determine whether it comes from Alice or another device (i.e., the attacker Eve). Bob estimates the CSI from the message and compares it with the CSI of the identification association step: if the two values match (according to a certain metric), the message is accepted as authentic, otherwise it is discarded as being fake. Bob repeats this step at each new message reception.

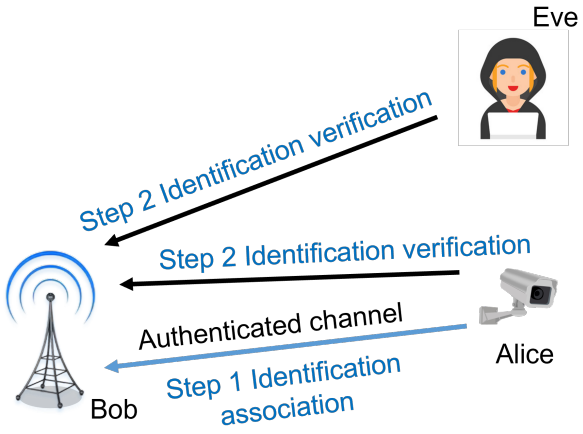

Figure 2. The TB PLS authentication scheme.

This strategy is suitable when the CSI is slowly time-varying, so its value will be considered unchanged in both steps.

Specific attacks against TB PLS authentication typically assume that Eve transmits (in Step 2) a suitably pre-coded signal such that Bob estimates a CSI predetermined by Eve. Note that in this case *multiple attacks* are possible, wherein Eve changes the precoding, to induce different CSI estimates at Bob, until a precoding passing the authentication verification is found. For an approach to optimize precoding over various attacks, see [14], where it is shown that TB PLS authentication can be broken with high probability with few attacks in a static scenario. Also, once a successful attack is found, it can be repeated indefinitely with success.

Challenge-Response PLS Authentication

We propose now a general framework for CR PLS authentication exploiting channels that are (partially) controllable by Bob. Our mechanism does not require an explicit secret shared between Alice and Bob, as the physical channel properties will be exploited to uniquely authenticate Alice. In the following, the *channel configuration* refers to a specific choice by Bob of the controllable channel parameters.

The CR PLS authentication protocol works as follows:

1) *Step 1, CSI measurements:* Alice transmits to Bob *several* pilot signals over the partially controllable channel, in correspondence to *several channel configurations* properly chosen by Bob; such transmissions are authenticated by higher-layer security mechanisms; Bob

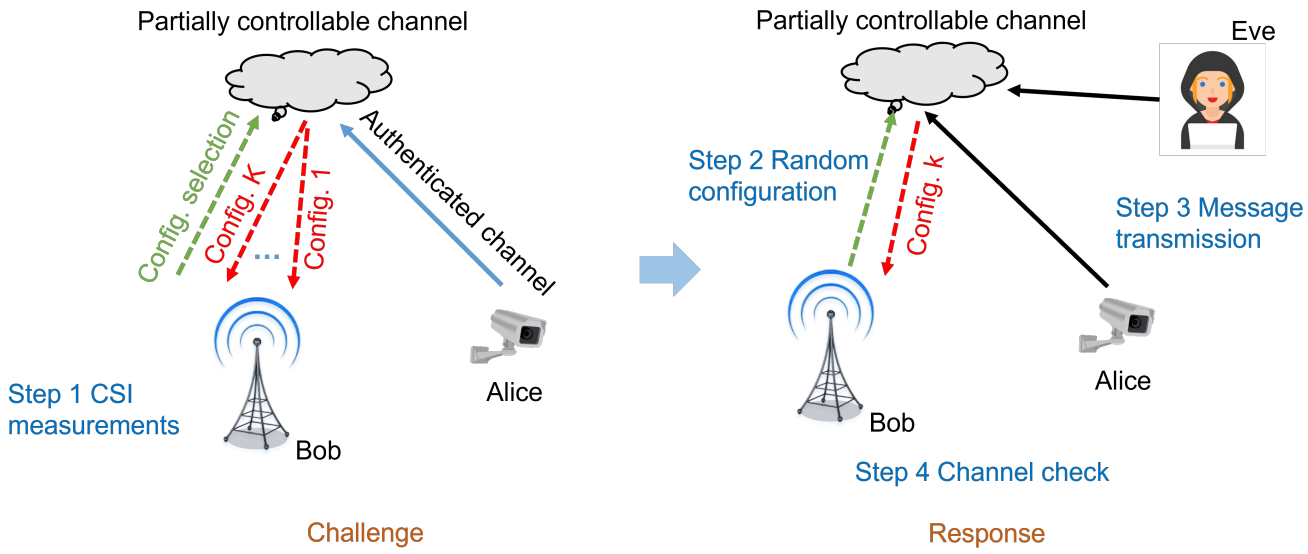

Figure 3. The CR PLS authentication scheme.

estimates the CSIs using the pilot signals and stores them, together with the used configurations.

2) *Step 2, random configuration:* Bob poses a challenge to Alice by randomly choosing a channel configuration; such configuration may have been already explored in Step 1 or not. In the latter case, Bob should be able to predict his resulting CSI to Alice, with the new configuration, based on the observations of Step 1.
3) *Step 3, message transmission:* Alice transmits the message and from the received signal Bob estimates the CSI, which represents the response from Alice;
4) *Step 4, channel check:* if the estimated CSI (response) matches the CSI predicted in Step 2 (expected response), Bob accepts the message as authentic.

This procedure does not leverage a pre-shared secret, except in Step 1, where authenticated signals must be transmitted: such an assumption is common also to the identification association step of TB PLS authentication. Moreover, the random channel configuration in Step 2 should be refreshed periodically, ideally at each new message transmission.

When compared to TB PLS authentication, the CSI measurements step corresponds to the identification association step, and the message transmission and CSI check steps correspond to the identification verification step. The random configuration step is unique to CR PLS authentication. CR PLS authentication includes TB PLS authentication as a subcase, where the challenge is always the same (i.e., Bob does not control the channel). However, the extension is not trivial, as the resulting mechanism is more secure, as shown in the following.

Due to the need to explore several configurations, the CSI measurements step takes more time and energy than the identification association step. Indeed, exploring a larger number of configurations both increases the protocol overhead and enlarges the domain of the random configurations used in Step 3, thus making the attack more difficult. Moreover, additional resources (in terms of time and energy) are also needed to configure the channel in Step 2. Lastly, the random channel configuration should still satisfy external constraints (e.g., on the communication quality) in Step 3; this may limit in practice the range of the random configuration.

Security Considerations

We now consider several threats and mitigation solutions using CR PLS authentication. We will mostly refer to the IRS example.

Multiple Attacks: TB PLS authentication is particularly vulnerable to multiple attacks, as described above and in [14]. Such a threat is considerably mitigated when using CR PLS authentication, as an effective attack should be based on the specific challenge, which is still not known to Eve. Moreover, even if an attack is successful, its repetition will typically not be successful with another configuration. Hence, although a successful attack reduces the security level, it still does not completely nullify it (as happens in TB PLS authentication).

Eve's Knowledge of the Effects of Control: A second threat occurs when Eve knows the effects of each control on the channel. In the IRS scenario, Eve knows either separately the CSI of the two Alice-IRS and IRS-Bob channels, or the resulting Alice-Bob CSI for each IRS configuration. Both cases are challenging, as the first typically requires ray tracing capabilities, while the latter is time consuming. In any case, the attack is more difficult than that against the TB PLS mechanism, where Eve needs to know only the overall Alice-Bob CSI. Moreover, even when Eve perfectly knows the effects on signal propagation of all configurations, CR PLS authentication is still effective, since Eve does not know the current channel configuration, and thus she does not know which is the successful attack.

Eve's Knowledge of the Channel Configuration: A third threat occurs when Eve knows the channel configuration. For example, Eve intercepts the control signal that re-configures

the IRS. This is a distinctive feature with respect to non-PLS CR authentication, where the challenge is public. Now, as long as Eve does not know the effects of the control on the CSI, the knowledge of the channel configuration makes multiple attacks more efficient (as they can be specialized for each configuration) but still CR PLS authentication is more secure than TB PLS authentication, as it takes more time to find the correct attack for *each* channel configuration. This attack can be mitigated by protecting the control signals with confidentiality mechanisms. Lastly, note that the knowledge of *both* the control *and* effects of the control render the authentication procedure ineffective.

Alteration of the Control Channel: If Eve is able to alter the control signals, she can reduce the randomness in the configuration to her advantage. Such a threat can be mitigated by protecting the control signals with integrity protection techniques.

Bypass of the Control Channel: If Eve transmits signals directly to the IRS, she only needs an estimate of the Alice-IRS channel to provide the correct response to Bob for any IRS configuration. In such a scenario, CR PLS authentication degenerates to TB PLS authentication: although several challenges (channel configurations) are started, the different responses (CSI values at Bob) are immediately available also to Eve. Still, Eve has to estimate the Alice-IRS CSI, with a complexity comparable to or higher – considering that the IRS may have a much larger number of elements than Bob's antennas and Eve has typically access only to signals received through the *cascaded* Alice-IRS-Eve channel – than that needed to estimate the Alice-Bob CSI in TB PLS authentication.

A New Channel Model For Security

The main property of partially controllable channels is their capability of being modifiable *without intervening* on the transmitted or received signals. Indeed, we observe that any processing at either the transmitter or the receiver modifies the equivalent baseband model. However, operations done at the receiver equally affect all received signals, thus they do not reveal anything about the transmitter or the channel itself and are not useful for authentication purposes. Operations done at the transmitter instead can be replicated by devices in any position, with the knowledge of the operation to be performed: therefore, using transmit operations to generate the proper response to a challenge requires either a pre-shared secret or a confidential transmission to share it. The first approach is the well-known CR authentication mechanism operating the higher network layer, while the latter approach is that of [3]. In this paper, we aim at obtaining the response directly from the channel, without transmitted or pre-shared secrets. Similarly, the mechanism of [5] for detecting sensor spoofing is operating at the transmitter, and indeed an attacker able to intercept this transmitted signal can disrupt the authentication mechanism.

More generally, the channel control should be relevant for authentication, i.e., the attack must also depend on the control itself to be effective. An example, wherein the control is not effective for authentication, occurs (in the IRS scenario) when Eve can transmit to Bob through the IRS, precoding her signal so that it reaches the IRS as it went through the Alice-IRS channel. As already observed, in this case any attack does not depend on the IRS configuration (the controllable part of the channel).

Moreover, we require that the control operated by Bob is not observable / identifiable by Eve, to prevent her from forging the expected CSI. This means that Eve does not know for example the IRS configuration or the positions of the drones in the swarm, otherwise she could infer the CSI and forge her attack accordingly.

For authentication purposes we want a *partial* controllability, as the CSI should be still in part random and depending on the position of transmitting / receiving devices or, in general, their features. This makes CSIs from Alice and Eve distinguishable to Bob. For example, Bob must control the IRS configuration, but not the channels to and from the IRS.

The partially controllable channel shares a few similarities with the *compound channel* model, where the channel belongs to a certain set of channel states (the uncertainty set). Such a set resembles that of configurations in a controllable channel; however, the main difference between the two models is that in controllable channels the configurations are *chosen* by Bob, while in compound channels the states are given by nature and are at most *known* to devices.

Controllable channels described in this section have been already exploited for communication purposes, However, in those applications, controllable devices were *adapted to* the electromagnetic environment [15] to improve coverage, while here we use them to *modify* the electromagnetic environment for authentication purposes. This in general yields a degradation of the communication performance, as discussed in the following.

Lastly, we should remark that in future networks there may not be a single entity controlling the infrastructure devices (IRSs, relays, and drones) as they can be partially adaptive or shared among multiple cells and not fully controlled by any of them; cell-free networks are also an extreme example of such scenario. This opens a gray area on the controllable and uncontrollable parts of the channel, as channel controllability may depend on the coordination of the different entities of the network, which deserves further study.

Performance Results

We consider a cellular network with an IRS having elements with unitary gain and fully controllable phases, organized at equally spaced positions along a line. Each device (Alice, Bob, and Eve) is equipped with a single antenna, providing a simple closed-form expression of IRS phases to maximize the resulting channel gain at Bob: we denote this as the *optimal IRS configuration*; note however that such optimality is for communication rather than authentication purposes. Narrowband channels among antennas and IRS elements are generated as independent Gaussian zero-mean unitary-power variables, and the channel between Alice and Bob is a complex number, whose noisy version represents the CSI estimated by Bob.

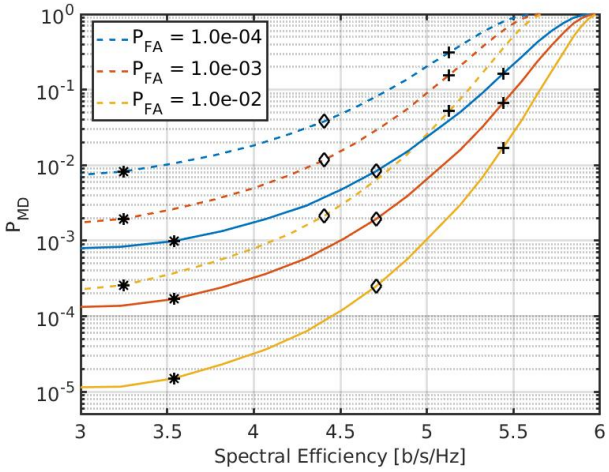

Figure 4. Misdetection probability of the authentication attack vs the spectral efficiency of the Alice-Bob communication link, obtained by varying the size of the angular interval of randomness of the IRS configuration, for IRSs of 100 (solid lines) and 80 elements (dashed lines). Cross, diamond, and star markers are set in correspondence of interval sizes $2\pi/3$, π, and $4\pi/3$, respectively.

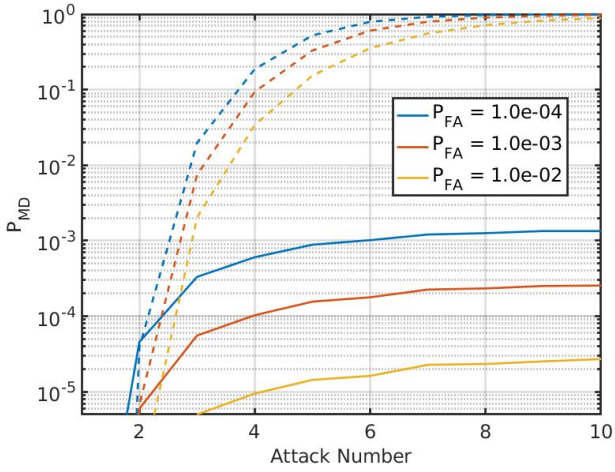

Figure 5. Misdetection probability vs the number of attacks, for TB (dashed lines) and CR (solid lines) PLS authentication methods. For CR PLS authentication, the angular interval size is $4\pi/3$. The IRS has 100 elements.

For CR PLS authentication, the phases (in radians) of the IRS elements are set uniformly at random in an angular interval (modulus 2π) around the optimal configuration, independently for each element. Note that, on one hand, a larger interval size increases the variance of the random IRS configuration, thus making the resulting CSI more diverse and less predictable. On the other hand, deviating from the optimal configuration reduces the signal-to-noise ratio (SNR) of the Alice-Bob link, thus reducing its spectral efficiency. This is an example of the trade-off between security and other performance metrics or external constraints.

For authentication we resort to the likelihood ratio test [14], with a threshold achieving a target false alarm (FA) probability. Eve does not know the IRS configuration but is assumed to perfectly know the CSI of the Alice-IRS and IRS-Bob channels, which is very favorable for her. As previously observed, even in such conditions, CR PLS authentication provides a stronger security than TB PLS authentication. Indeed, the shared secret for CR authentication is only the IRS configuration. Eve cannot transmit messages to Bob through the IRS, but she can only send messages directly to Bob, over a channel forged for the maximum probability of success; thus she transmits messages to Bob as they are going through the average Alice-Bob channel, where the mean is taken over all IRS configurations, assumed to be taken with the same probability, [14].

Fig. 4 shows the misdetection (MD) probability (i.e., the probability of wrongly authenticating a message coming from Eve) as a function of the spectral efficiency of the Alice-Bob communication link, obtained by varying the size of the interval for the random phase of each IRS element around the optimal configuration. Two sizes of IRS are considered: 100 elements (solid lines) and 80 elements (dashed lines), and three values of the target FA probability ($10^{-2}, 10^{-3}$, and 10^{-4}) are considered. We observe that a larger interval size significantly reduces the MD probability, and that with a reduction of spectral efficiency of 3 b/s/Hz we already obtain an MD probability in the range 10^{-5} to 10^{-3}, depending on the imposed FA probability. Note also that, since we assume that Eve knows the CSIs of the Alice-IRS and IRS-Bob channels, the attack is highly successful (i.e., the MD probability is close to 1) in the absence of randomization of the IRS element phases (top right of the figure), yielding in turn the maximum spectral efficiency. This extreme case is the state-of-the-art TB PLS authentication, under the unfavorable conditions of CSIs known to Eve.

We also investigate the case wherein Eve does not have perfect knowledge of the CSIs of channels between the IRS and Alice / Bob, but she has estimates corrupted by additive white Gaussian noise (AWGN). We compare CR and TB PLS authentications, where the latter uses the optimal IRS configuration (i.e., the random interval has zero size). At each attack, we assume that Eve obtains a new estimate of the channels, which can be averaged with the previous estimates to forge better CSI for the next attacks; note that better channel estimates not only provide a better estimate of the Alice-Bob CSI, but they also yield a better estimate of the IRS configuration, which in turn further improves the Alice-Bob CSI estimate.

From Fig. 5 we observe that for state-of-the-art TB PLS authentication the channel estimate is so good after a few attacks that the MD probability quickly approaches 1. With the new CR PLS authentication instead, even with a large number of observations, the MD is still kept below 10^{-3}, thanks to the randomness introduced by changing the IRS configuration. As expected, CR PLS authentication is able to neutralize multiple attacks, with a significant advantage over the current TB PLS authentication.

Open Research Challenges

Several research challenges remain open when considering CR PLS solutions based on partially controllable channels:

- The security performance should be assessed in various specific contexts (e.g., using IRSs, relays, and drone

swarms), and implementation challenges should be addressed.
- CR PLS authentication should be accurately analyzed based on information theoretic tools to better understand the achievable security-communication trade-off, as that considered in Fig. 4.
- New attacks and countermeasures should be considered for CR PLS authentication over partially controllable channels, as the attacker may infer the channel configuration or perform more efficient multiple attacks based on its partial knowledge.
- Theoretical and implementation connections with other security mechanisms, such as those based on PUFs should be investigated, to merge them into stronger authentication solutions.
- The use of partially controllable channels for other security targets beyond authentication should be addressed to exploit the potential of future communication systems for stronger security.
- The use of controllable channels for attack purposes should be considered, in particular when targeting authentication mechanisms, e.g., when IRSs or relays are deployed by the attacker (as considered in a PLS confidentiality scenario in [8]).
- As already mentioned, networks with partial control of the infrastructure require new solutions to properly integrate CR PLS authentication, possibly calling for a tighter coordination of the network components.

BIOGRAPHIES

Stefano Tomasin (stefano.tomasin@unipd.it) is a Full Professor at the University of Padova, Italy. His interests include signal processing for communications and physical layer security. Since 2011 he has been an Editor of EURASIP Journal of Wireless Communications and Networking and since 2020 Editor of the IEEE Transactions on Information Forensics and Security.

Hongliang Zhang (hz16@princeton.edu) is a postdoctoral associate in the Department of Electrical and Computer Engineering at Princeton University. He was the recipient of the 2021 IEEE Comsoc Heinrich Hertz Award.

Arsenia Chorti (arsenia.chorti@ensea.fr) is a Professor at the École Nationale Supérieure de l'Électronique et de ses Applications (ENSEA), Joint Head of the ICI Group of the ETIS Lab UMR 8051, Leader of the Wireless Connectivity group of the Barkhausen Institute and Visiting Scholar at Princeton and Essex Universities. Her research spans the areas of wireless communications and wireless systems security for 5G and 6G. She is a Senior IEEE Member, member of the IEEE INGR on Security while since October 2021 she is chairing the IEEE Focus Group on Physical Layer Security.

H. Vincent Poor (poor@princeton.edu) is the Michael Henry Strater University Professor at Princeton University, where his interests include wireless networks and related fields. A member of the U.S. National Academies of Engineering and Sciences, he received the IEEE Alexander Graham Bell Medal in 2017.

REFERENCES

[1] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. CRC Press, 2013.

[2] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 282–310, 1st Quart. 2021.

[3] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1817–1827, Sep. 2013.

[4] X. Wu, Z. Yang, C. Ling, and X.-G. Xia, "Artificial-noise-aided physical layer phase challenge-response authentication for practical OFDM transmission," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6611–6625, Oct. 2016.

[5] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "PyCRA: Physical challenge-response authentication for active sensors under spoofing attacks," in *Proc. ACM SIGSAC CCS*, Denver, CO, USA, Oct. 2015.

[6] X. Lu, L. Xiao, T. Xu, Y. Zhao, Y. Tang, and W. Zhuang, "Reinforcement learning based PHY authentication for VANETs," *IEEE Trans. on Vehicular Tech.*, vol. 69, no. 3, pp. 3068–3079, 2020.

[7] A. Chorti, A. N. Barreto, S. Köpsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, and H. V. Poor, "Context-aware security for 6G wireless: The role of physical layer security," *IEEE Commun. Stand. Mag.*, vol. 6, no. 1, pp. 102–108, 2022.

[8] Y. Wang, H. Lu, D. Zhao, Y. Deng, and A. Nallanathan, "Wireless communication in the presence of illegal reconfigurable intelligent surface: Signal leakage and interference attack," *IEEE Wireless Commun.*, to be published.

[9] R. Flamini, D. De Donno, J. Gambini, F. Giuppi, C. Mazzucco, A. Milani, and L. Resteghini, "Towards a heterogeneous smart electromagnetic environment for millimeter-wave communications: An industrial viewpoint," *IEEE Trans. Antennas Propag.*, to be published.

[10] M. Mitev, M. Shakiba-Herfeh, A. Chorti, and M. Reed, "Multi-factor physical layer security authentication in short blocklength communications," *IEEE Access*, to appear.

[11] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, "Physical layer security in UAV systems: Challenges and opportunities," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 40–47, Oct. 2019.

[12] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[13] G. Amarasuriya, R. F. Schaefer, and H. V. Poor, "Linear precoder design for physical layer security via reconfigurable intelligent surfaces," in *Proc. IEEE SPAWC*, Atlanta, GA, USA, May 2022.

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

[15] H. Zhang, S. Zeng, B. Di, Y. Tan, M. Di Renzo, M. Debbah, Z. Han, H. V. Poor, and L. Song, "Intelligent omni-surfaces for full-dimensional wireless communications: Principles, technology, and implementation," *IEEE Commun. Mag.*, vol. 60, no. 2, pp. 39–45, Feb. 2022.