2024 European Control Conference (ECC)
June 25-28, 2024. Stockholm, Sweden

A Moving Target Defense Mechanism based on Spatial Unpredictability for Wireless Communication

Aris Kanellopoulos, Christos Mavridis, Ragnar Thobaben, and Karl Henrik Johansson

Abstract— **In this paper we propose an unpredictability-based jamming defense framework based on the principles of Moving Target Defense for a wireless communication problem. Taking advantage of the complex nature of large-scale cyber-physical systems, we consider a platform consisting of a single receiving component but multiple potential transmitting components, each equipped with a multi-antenna phased array. We formulate an optimization problem over the probability simplex that characterizes a randomized receiving angle which seeks to balance between the estimated performance of the transmission and an entropy-based unpredictability measure. Furthermore, we explore the effect of an intelligent adversary that has knowledge of the derived probabilities and optimally places a single-antenna jamming device to disrupt the communication links. Finally, simulation results showcase the efficacy of the proposed algorithm.**

I. Introduction

Cyber-physical systems (CPS) are becoming ubiquitous in a variety of application domains, both in civilian and military life, such as healthcare, smart grids and unmanned vehicles. These systems consist of physical components, often ones with limited capabilities, connected and communicating over complex networks. Even though they potentially lack computational capabilities, CPS often include low-cost components, which facilitate design of large-scale, complex systems [1].

The compositionality and complexity that characterize CPS are also the sources of their greatest drawback; their susceptibility to external manipulation, whether this is stochastic or adversarial in nature. Consequently, the problem of robustifying and defending CPS against attackers has been at the forefront of a plethora of research communities. From a computer engineering perspective, scholars have focused on designing protocols that shield systems against system intruders on the software level [2]. On the other hand, control theory has been introduced in CPS security problems as tools to tackle the issue from the hardware side; proposing algorithms that guarantee continuous operation of the system even under malicious influence [3]. Finally, research has been conducted on the problem of securing CPS whose underlying component connection network has been compromised [4]. These approaches often rely on graph-theoretic tools that do not model the actual communication interfaces of the various subsystems in a CPS. A consideration that permeates the aforementioned approaches to CPS security is the need to accurately construct a predictive model of the adversary's behavior. Game theory and optimization approaches has been used for such purposes, where different solution concepts have been applied and investigated, ranging from Nash equilibrium strategies to worst-case attack scenarios [5].

Although, as mentioned, there has been extensive research on attacks to the communication substrata of CPS, the relevant communities have not yet focused on the physical properties of the network, e.g., on injections to the wireless signals connecting the CPS components, as well as the defense design opportunities that arise due to the specific nature of CPS, i.e., their low-cost devices and their complexity. In this work, we propose a security framework that employs models of wireless communications and which rests on ideas of component redundancy and behavior unpredictability to shield the system.

To this end, we introduce the framework of Moving Target Defense (MTD), a security strategy that increases the complexity and the unpredictability of the system by dynamically shifting its configuration, thereby increasing its attack surface [6]. MTD methods have been utilized in different scenarios, whereas lately they have been introduced to the CPS literature [7]. The underlying principle of operation of the proposed scheme is the exploitation of the directionality of wireless signals in modern communication devices by randomly changing the transmitting subsystem to a designated component. Beamforming methods can be employed in order to select the received signal direction at each transmission time [8]. While the defense strategy of the CPS is designed to be agnostic to the attacker, we further investigate potential attacks and characterize the worst-case behavior of an intelligent adversary that has knowledge of the parameters of the security protocol.

A. Related Work

The problem of securing CPS has been explored from researchers in a variety of fields of study. The authors of [9] indicated the importance of investigating CPS security from different points of view and utilizing approaches from different disciplines. Accordingly, the authors of [10] present an overview of methods that robustify consensus algorithms in networks of communicating agents using tools from graph theory. Moreover, different control methodologies, such as Model Predictive Control [11] have been co-designed with the security problem in mind via homomorphic encryption methods. Finally, from the perspective of the physical domain, the authors of [12] investigate game-theoretic methods of mitigating stealthy attacks that are designed in a receding-horizon fashion.

The authors are with the School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Stockholm. emails:{arisk,mavridis,ragnart,kallej}@kth.se.

This work was supported in part by the Swedish Civil Contingencies Agency through the CERCES2 project.

Securing the physical layer of wireless communications is a well-studied problem. In [13], the authors propose an optimization-based method of estimating a jammer's characteristics as well as mitigating their effect on a wireless transmission. In similar settings, research has been conducted on the use of intelligent reflective surfaces for wireless security [14] as well as on the effects of novel technologies, such as mmWave communications, on security and privacy system requirements [15].

Unpredictability-based MTD frameworks were initially designed for computer networks [16]–[18]. In [19], the authors apply the principles of MTD to constantly rotating Internet Protocol version 6 (IPv6) addresses. A more rigorous mathematical approach to MTD was introduced in [20], that led to an entropy hypothesis framework that has been applied to different scenarios. As an example, in [7], a CPS with redundant sensing and actuating components is considered, which employs a randomized switching strategy over its potential observers and controllers.

B. Contribution

The contribution of this paper is threefold. Firstly, we utilize tools from wireless communications to model the channels between the multi-antenna receiver, the various transmitters and a potential single-antenna jamming device. Subsequently, we derive the probabilities of communicating with a specific transmitter based on an unpredictability-based, MTD framework. Finally, we present a worst case attack from the perspective of an adversary who has knowledge of the MTD strategies.

a) Notation: The notation we use in this paper is standard. For a complex matrix $A \in \mathbb{C}^{n\times m}$, we denote by $\bar{A} \in \mathbb{C}^{n\times m}$ its complex conjugate and by $A^{\mathrm{H}} \in \mathbb{C}^{m\times n}$ its Hermitian. Similarly, $A^{\mathrm{T}} \in \mathbb{C}^{m\times n}$ is the transpose of A. Furthermore, $\|A\|$ is the norm of A – defined appropriately – while in the case that $n = 1$, then the absolute value of the complex scalar is denoted by $|A|$. The maximum eigenvalue of A is denoted as $\bar{\lambda}(A)$ and the associated eigenvector $\bar{v}(A)$ such that $A\bar{v}(A) = \bar{\lambda}(A)\bar{v}(A)$. The identity matrix of appropriate dimensions is denoted as I. We denote the n-dimensional simplex as Δ^n and, finally, to facilitate the readers when needed, we denote the exponential function as $\exp(x) = e^x$.

b) Structure: The paper is structured as follows. In Section II, we model the wireless communication channels between the spatially distributed system components and the jamming device based on their geometric characteristics and we describe communication-theoretic performance metrics. Section III formulates the MTD optimization problem and highlights its solution. Section IV discusses the worst-case behavior of an attacker that has knowledge of the MTD strategy. Finally, Section V presents simulation results that showcase the efficacy of the approach while Section VI concludes the paper and proposes potential future research directions.

II. Problem Formulation

Consider a region $\mathcal{R} \subset \mathbb{R}^2$. Within $\mathcal{R}$, there are N transmitting devices that serve a receiving component, or user. Typically, the system designer would consider quality of service and transmission rate as the only requirement in determining which transmitter would serve the receiver. However, in this work, we will investigate a proactive method of defending the system against jamming attacks by allocating transmitters to the receiver based on the principles of MTD. These algorithms comprise a class of defense approaches that rest on rendering the system unpredictable in its behavior, and thus, hindering the attacker.

Assuming uniform linear array (ULA) antennas, the channel between the targeted receiver and the i-th transmitter is denoted by $H_i \in \mathbb{C}^{M_r\times M_t^i}$ and is modeled, according to [21], as

$$H_i = \sum_{l=1}^{L_i} \bar{a}_i \exp\Big(-\frac{j2\pi d}{l_c}\Big)\alpha_r(\theta_i^r)\alpha_t^{\mathrm{H}}(\theta_i^t), \qquad (1)$$

where $\bar{a}_i \in \mathbb{R}$ is the distance-dependent path-loss between the transmitter and the receiver, $d \in \mathbb{R}$ the antenna separation, $l_c \in \mathbb{R}$ the wavelength of the carrier signal and L_i the number of paths.

Remark 1: Without loss of generality, for ease of exposition we let $L_i = 1,\ \forall i$, i.e., we consider line-of-sight (LoS) channels between all devices. Our results are readily extended to the case of multi-path transmissions, although stochastic models of channel properties will need to be considered.

The spatial signatures of the channel in the transmit and receive direction are denoted as $\alpha_r(\theta_i^r) \in \mathbb{C}^{M_r}$ and $\alpha_t(\theta_i^t) \in \mathbb{C}^{M_t^i}$, respectively. It holds that

$$\alpha_r(\theta_i^r) = \frac{1}{\sqrt{M_r}}\left[1, e^{j(2\pi/l_c)d\Omega_i^r}, \cdots, e^{j(2\pi/l_c)d(M_r-1)\Omega_i^r}\right],$$

where $\Omega_i^r = \sin(\theta_i^r)$. Similarly, the spacial signature in the transmit direction is given as

$$\alpha_t(\theta_i^t) = \frac{1}{\sqrt{M_r^i}}\left[1, e^{j(2\pi/l_c)d\Omega_i^t}, \cdots, e^{j(2\pi/l_c)d(M_t^i-1)\Omega_i^t}\right],$$

where $\Omega_i^t = \cos(\theta_i^t)$. Furthermore, we consider a communication system under attack by an adversarial agent who is able to place a single-antenna jamming device near the receiver of the targeted user. The channel between the jammer and the user, denoted as $h_a \in \mathbb{C}^{M_r}$, is modeled in a fashion similar to (1).

The transmitting i-th device, precodes a transmitted symbol $s \in \mathbb{C}$ with unit power via a beamforming vector $W_i \in \mathbb{C}^{M_t^i}$. As such, the transmitted signal from the transmitter becomes $x = W_i s \in \mathbb{C}^{M_t^i}$. The total received signal at the user, $y \in \mathbb{C}^{M_r}$, is

$$y = H_i W_i s + \eta, \qquad (2)$$

where $\eta \in \mathbb{C}^{M_r}$ is the random noise of the transmission, modeled as a Gaussian random variable with $\|\eta\| = \sigma$.

Finally, after receiving the signal, the user decodes it via a receive combiner $F_i \in \mathbb{C}^{M_r}$.

Remark 2: The design of the transmit and receive beamforming vectors, W_i and F_i, are well-studied problems in the communication literature and go beyond the scope of this work. We note that our proposed algorithms do not depend on this design.

Subsequently, the signal-to-noise ratio (SNR) of the received signal is defined as

$$\gamma_i = \frac{|F_i^{\mathrm{H}} H_i W_i|^2}{\sigma^2}. \tag{3}$$

Since the SNR can be used as a measure of the quality of the communication system, it is natural for the transmission to take place between the receiver and the transmitter that maximizes it; i.e., with the device that offers better channel quality. Thus, the optimal SNR is given as $\gamma^\star = \max_i \gamma_i$, and defines the transmitter that is better located to service intended device.

In the simplified – but realistic in the case of high-frequency communication systems – channel models we have described in this work, it is clearly seen that both the distance of the receiver to the servicing transmitter and the relative angle between the two affects the channel characteristics. As such, it would be expected that a stationary user is best serviced by the same transmitter at all times. However, this level of predictability in the transmission scheme can be detrimental in adversarial environments. In order to investigate the effects of an adversary that tries to compromise the DL transmission, we consider the existence of a single-antenna jamming device in $\mathcal{R}$, whose channel to the user is denoted by h_a. We note that if θ_a is the angle of arrival of the signal from the jammer to the user, then it holds that

$$h_a = \bar{a}_a \exp\left(-\frac{j2\pi d}{l_c}\right)\alpha_r(\theta_a).$$

The jamming signal transmitted is denoted as $\delta \in \mathbb{C}$ such that $\|\delta\| = 1$ without loss of generality while the total received signal now becomes

$$y = H_i W_i s + h_a \delta + \eta. \tag{4}$$

A metric of the performance of the transmission in this case is the signal-to-noise and interference-ratio (SINR), which is defined as

$$\gamma_i^a = \frac{|F_i^{\mathrm{H}} H_i W_i|^2}{\sigma^2 + |F_i^{\mathrm{H}} h_a|^2}. \tag{5}$$

Remark 3: Although we consider LoS channels with known parameters throughout the design of our unpredictability-based defense algorithm for clarity of exposition, our results are applicable to more complex environments where multi-path fading and non-LoS channels can be considered. Communication protocols already contain channel estimation periods – via pilot signals – which allow the network to compute estimates of the channel information itself, as well as the expected SNRs for specific links.

It can now be seen that the SINR is a function of the choice of transmitter with which the device will communicate – indicated by the integer $i \in \{1, \ldots, N\}$ – as well as the placement of the jamming device by the attacker, which defines the properties of the channel via h_a. Given deterministic knowledge of the servicing component, the attacker can place the jamming device in an optimal position that minimizes γ_i^a with respect to h_a; in LoS cases, this is located as close to the receiver as possible and in the same direction as the legitimate angle of arrival. To mitigate this, we propose an unpredictability-based mechanism where the choice of servicing transmitter becomes probabilistic, based on the solution of an optimization problem considering both the expected performance of the communication system and the unpredictability of its operation. Furthermore, we explore the worst-case placement of the jamming device in the case of an adversary that has knowledge of the MTD algorithm. An overview of the considered scenario is shown in Fig. 1.

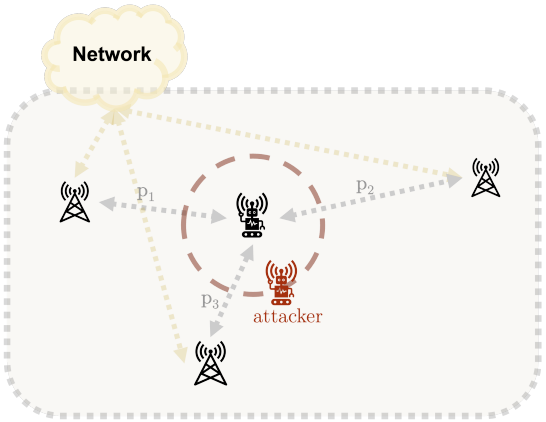

Fig. 1: Illustration of the problem configuration.

III. Moving-Target Defense Mechanism

In this section, we formulate an optimization problem via which the legitimate users of the communications system can derive a probabilistic in space transmission scheme; i.e., a system shielding mechanism that incorporates the same principles of MTD that have been extensively used in approaches such as frequency hopping. Specifically, we allow the user and the legitimate transmitters to partly sacrifice the performance of the communication system in order to achieve higher security capabilities by randomly choosing the active sender, instead of employing only the one that is optimally located with respect to the user. Due to the high directionality of the multi-antenna systems investigated – especially in higher frequencies – it will be shown that by increasing the probability that the jammer is placed in different angle than the transmitter, the system can increase the performance under attack.

We note that in accordance with the principles of MTD, our first proposed algorithm is agnostic to the existence of the attacker. Consequently, it can be implemented for any system *a priori*, achieving a balance between expected performance loss and gain in defensive capability.

Initially, we let $p \in \Delta^N$ denote a vector whose elements p_i correspond to the probability of the device communicating with the i-th transmitter. However, instead of arbitrarily and uniformly choosing a transmitting direction, we define an optimization problem that balances between the transmission strategy that maximizes the performance of the system and the one that is most unpredictable. The formulation of this problem, then, becomes:

$$\max_{p\in\Delta^N}(1-\epsilon)\mathbb{E}_{q\sim p}[\gamma]+\epsilon\mathcal{H}(p), \tag{6}$$

where $\epsilon \in \mathbb{R}^+$ is a designer parameter that denotes the level of unpredictability of the system operation and $\mathcal{H}(q) = -q^{\mathrm{T}}\log(q)$ is the entropy induced by a probability $q \in \Delta^N$.

Remark 4: We follow previous works on MTD [7] in defining the induced entropy to be the unpredictability metric of the optimization problem. This approach has been one of the most rigorous in terms of mathematically describing the effects of MTD in a system.

Theorem 1: Given the communication system described by the channel models (1) and SNRs defined as (3), then the optimal MTD strategy given the reward function (6) is achieved by the probability vector with elements

$$p_i^\star = \frac{\exp\left(\frac{(1-\epsilon)\gamma_i}{\epsilon}\right)}{\sum_{j=1}^N \exp\left(\frac{(1-\epsilon)\gamma_j}{\epsilon}\right)}. \tag{7}$$

Proof: The proof of the theorem follows from standard optimization results and it follows closely [7]. ∎

IV. MTD Against Intelligent Attackers

In the preceding chapter, we focused on an attacker-agnostic model, in which the actual impact of the adversary's behavior to the system, as well as their potential knowledge of the MTD algorithm are not considered. In the sequel, we will employ optimization tools in order to explore the interaction between an MTD strategy and a rational malicious agent who takes into account the randomized nature of the transmissions when placing the jamming device. Consequently, we will be able to quantify the effect of the MTD strategy against a worst-case attacker.

In order to properly investigate the effect of the attacker, and to facilitate the reader, we let the action set of the attacker to be, without loss of generality, the set of normalized channels $h_a \in \mathbb{C}_a^N$. As far as the adversary is concerned, in this way we let them arbitrarily place the jamming device at an angle θ_a at a fixed distance around the user. It has been shown that there is a direct correspondence between the angle of arrival of the signal and the channel vector. Thus, by optimizing the channel vector itself, the attacker can easily find the optimal placement angle. Interested readers are referred to chapter 7 of [21] and the discussion about angular representations of channels therein.

Finally, for a given MTD strategy, i.e., a given probability $p_i^\star$ over $\mathcal{A}_d$, the worst-case attack is given with respect to the expected SINR defined in (5) as

$$\begin{aligned} J_a(\theta_a) &= \sum_{i=1}^N p_i^\star \gamma_i^a(\theta_a) \\ &= \sum_{i=1}^N p_i^\star \frac{|F_i^{\mathrm{H}} H_i W_i|^2}{\sigma^2 + |F_i^{\mathrm{H}} h_a(\theta_a)|^2}, \end{aligned} \tag{8}$$

where the explicit dependence on θ_a is emphasized.

Derivation of the optimal attack strategy rests on the solution of an optimization problem defined with respect to the function (8). However, this reward function is a sum of fractions that the attacker aims to minimize and, therefore, the optimization problem is non-trivial. While there is rich literature in fractional programming [22], for the purposes of exposition, we simplify the problem by considering the maximization from the attacker's perspective of the reciprocal of the SINR. Intuitively, the attacker aims to maximize the effect of the injected power to the system – quantified by the denominator of (8) – over the power of the legitimate signal – which is captured by the numerator.

Consequently, the optimization problem that the attacker considers becomes

$$\begin{aligned} J_a(\theta_a) &= \sum_{i=1}^N p_i^\star \gamma_i^a(\theta_a) \\ &= \sum_{i=1}^N p_i^\star \frac{|F_i^{\mathrm{H}} H_i W_i|^2}{\sigma^2 + |F_i^{\mathrm{H}} h_a(\theta_a)|^2}, \end{aligned} \tag{9}$$

Thus, we state the following theorem that characterizes the worst-case channel for the placement of the jamming device.

Theorem 2: Consider the communication system described by (4), operating under the MTD scheme with probabilities given by (7) and the associated SINR (5). Then, the optimal channel of the attacker's placement of a single-antenna jamming device is given as

$$h_a^\star = \bar{v}\left(\sum_{i=1}^N \frac{p_i^\star(\sigma^2 I + F_i^{\mathrm{H}} F_i)}{|F_i^{\mathrm{H}} H_i W_i|^2}\right).$$

Proof: As mentioned, we consider the following simplified problem for the adversary:

$$\begin{aligned} \max_{h_a} \bar{J}(h_a) = \max_{h_a} \sum_{i=1}^N \frac{p_i^\star(\sigma^2 + |F_i h_a|^2)}{|F_i^{\mathrm{H}} H_i W_i|^2}, \\ \text{subject to } \|h_a\| = 1. \end{aligned}$$

We rewrite the objective function, noting that, since h_a is a unit vector $\sigma^2 + |F_i h_a|^2 = h_a^{\mathrm{H}}(\sigma^2 I + F_i^{\mathrm{H}} F_i) h_a$. Thus, moving the optimization variables out of the summation, we have that

$$\max_{h_a} \bar{J}(h_a) = \max_{h_a} h_a^{\mathrm{H}}\left(\sum_{i=1}^N \frac{p_i^\star(\sigma^2 I + F_i^{\mathrm{H}} F_i)}{|F_i^{\mathrm{H}} H_i W_i|^2}\right) h_a,$$

subject to the channel vector lying in the N_r-dimensional unit sphere. Finally, note that the kernel matrix of the derived quadratic form is positive definite, and thus, by definition,

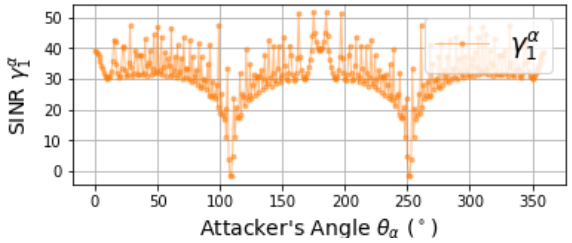

Fig. 2: SINR of the communication link between the receiver and the transmitter $i = 1$ as the angle of the jamming device changes.

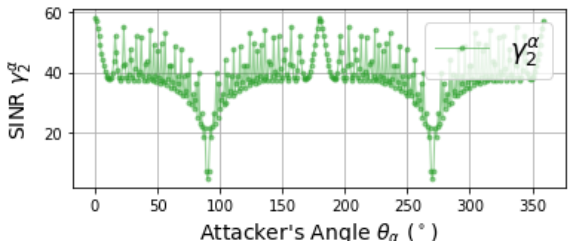

Fig. 3: SINR of the communication link between the receiver and the transmitter $i = 2$ as the angle of the jamming device changes.

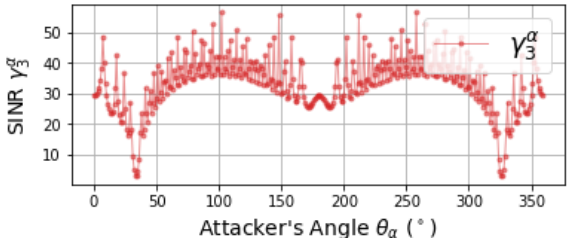

Fig. 4: SINR of the communication link between the receiver and the transmitter $i = 3$ as the angle of the jamming device changes.

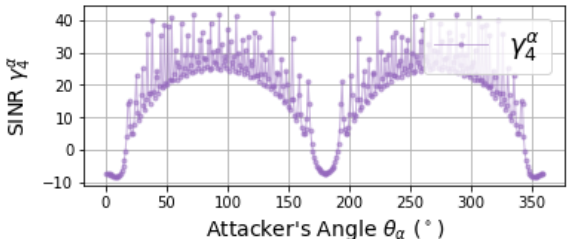

Fig. 5: SINR of the communication link between the receiver and the transmitter $i = 4$ as the angle of the jamming device changes.

the solution to the maximization problem is the eigenvector corresponding to the maximum eigenvalue of the matrix, i.e.,

$$h_a^\star = \bar{v}\left(\sum_{i=1}^{N} \frac{p_i^\star(\sigma^2 I + F_i^{\mathrm{H}} F_i)}{|F_i^{\mathrm{H}} H_i W_i|^2}\right),$$

which completes the proof. ■

V. Simulation Results

As is expected, the employment of a probabilistic transmission policy, leads to degradation of the performance of the communication system. By forcing the device to receive information from transmitters that are placed further away or – in more realistic environments – in more cluttered areas, the rate of the transmissions is expected to decrease. Simultaneously, the unpredictability gained by the MTD mechanism increases the security capabilities of the system. In this subsection, we investigate the efficacy of the MTD system theoretically by considering appropriate measures of performance and security for this system.

Initially, we examine the use of the MTD algorithm in the absence of attackers. In order to quantify the communication performance of the system, we utilize the expected SNR (without interference from an attacker) and measure the effect of the randomized strategy. By changing the level of unpredictability required by the MTD, i.e., the parameter ϵ, the resulting probability $p^\star$ changes following (7). The expected SNR then can be computed by the following:

$$\mathbb{E}_{q\sim p^\star(\epsilon)}[\gamma] = \sum_{i=1}^{M} \gamma_i p_i^\star(\epsilon), \tag{10}$$

where the functional dependence of $p_i^\star$ on ϵ is emphasized.

The studied system consists of $N = 4$ transmitters and an receiving devices communicating at 1GHz, i.e., with $f_c = 10^9$. Each device is equipped with an antenna array with 50 critically-spaced elements with $l_c = \lambda_c/2$. Given the positions $q_1, q_2 \in \mathcal{R}$ of two devices, the distance-dependent component of the path-loss $\bar{a}$ is modeled as $\bar{a} = \|q_1 - q_2\|^{-2}$. These values are computed according to the positions of the receiver $q_r = [2\ 6]^{\mathrm{T}}$, and the transmitters $q_1^t = [0\ 0]^{\mathrm{T}}$, $q_2^t = [2\ 3]^{\mathrm{T}}$, $q_3^t = [5\ 8]^{\mathrm{T}}$, and $q_4^t = [15\ 4]^{\mathrm{T}}$. Since the single-antenna attacker must be placed as close as possible to the receiving antenna to maximize the power of their injected interference, we bound their movement on a circle around the receiver of radius 0.1.

Accordingly, in Fig. 6 we can see the SNR levels of communicating with the different transmitters. It can thus be observed that the optimally placed transmitting device is the one indexed by $i = 1$ while the least favorable one is given for $i = 3$. Upon employment of the MTD strategy, the expected SNR is computed according to (10). With the increase of the unpredictability parameter ϵ, i.e., by making the communication scheme more unpredictable, we note the decreasing trend of the expected SNR. Specifically, for lower values of unpredictability, the system tends to select the optimal transmitting component deterministically. As the MTD scheme becomes more prevalent, the probability of communicating with a "worse" device becomes higher, until the limiting case, where the probability is uniform and the expected SNR is the average of the performance rates of the available transmitters.

Subsequently, we consider the same communication environment including an adversarial jammer. In Figures 2 to 5, we showcase the importance of the angle of placement of the jamming device (in a specific radius around the receiver). Specifically, we consider a jamming device statically placed at different angles, and for which it can be seen that depending on the transmitter chosen, the performance of the reception can vary.

Finally, in Fig. 7 we showcase the effects of the MTD

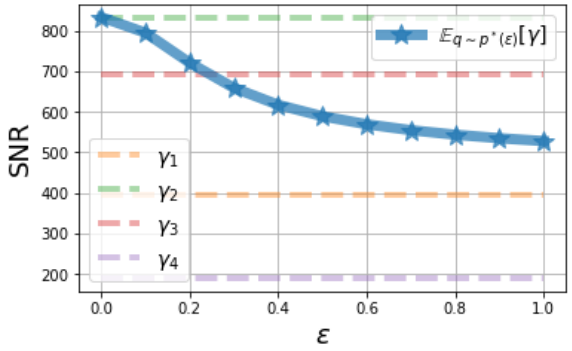

Fig. 6: Expected SNR of the communication link as ϵ increases and the MTD scheme becomes more randomized. The SNR for each transmitter is also highlighted

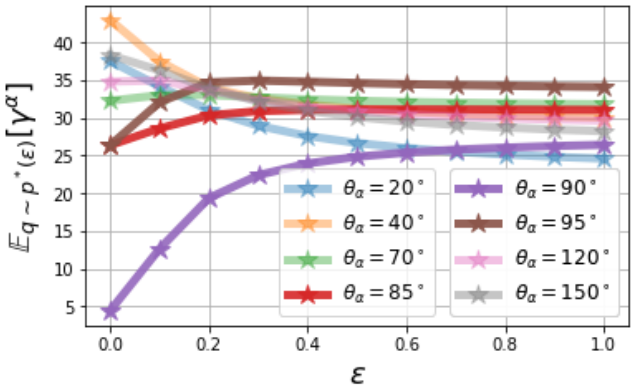

Fig. 7: Expected SINR for a system under jamming attack as the unpredictability weight is increased. We further highlight the performance of the system for different angles of jammer placement.

strategy in the presence of an attacker. It can thus be seen that while the MTD algorithm induces performance losses due the enforced communication with suboptimal transmitters, it is advantageous in the presence of a well-placed attacker, as it can be seen by the increase in performance as the unpredictability increases in the case of $\theta_a = \frac{\pi}{2}$, as is the

VI. Conclusion and Future Work

We proposed a defense mechanism based on the unpredictability principles of MTD. We considered a data transmission scenario involving a single receiver and multiple potential transmitters. The channels between the components were modeled using their geometric properties and with LoS consideration. An attacker agnostic randomized transmission scheme was designed based on an unpredictable change of the combiner of the receiver. Finally, we investigated the effects of an intelligent attacker that has access to the MTD strategy and can place a single antenna jamming device near the receiver. Simulation results showcased the balance between the robustness of the transmission via the increase in the expected SINR, and the performance with respect to the nominal operation of the system.

Future work will focus on allowing the receiver and the adversary to move within the region, and the design of an adaptive MTD policy against an intelligent attacker using game theoretic results.

References

[1] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution," in *Proceedings of the 47th design automation conference*. ACM, 2010, pp. 731–736.

[2] M. M. Alani and M. Alloghani, "Security challenges in the industry 4.0 era," *Industry 4.0 and engineering for a sustainable future*, pp. 117–136, 2019.

[3] H. Sandberg, S. Amin, and K. H. Johansson, "Cyberphysical security in networked control systems: An introduction to the issue," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 20–23, 2015.

[4] H. Sadreazami, A. Mohammadi, A. Asif, and K. N. Plataniotis, "Distributed-graph-based statistical approach for intrusion detection in cyber-physical systems," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 137–147, 2017.

[5] S. R. Etesami and T. Başar, "Dynamic games in cyber-physical security: An overview," *Dynamic Games and Applications*, vol. 9, no. 4, pp. 884–913, 2019.

[6] S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang, and X. S. Wang, *Moving target defense: creating asymmetric uncertainty for cyber threats*. Springer Science & Business Media, 2011, vol. 54.

[7] A. Kanellopoulos and K. G. Vamvoudakis, "A moving target defense control framework for cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 65, no. 3, pp. 1029–1043, 2019.

[8] J. Zhang, X. Yu, and K. B. Letaief, "Hybrid beamforming for 5g and beyond millimeter-wave systems: A holistic view," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 77–91, 2019.

[9] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on*. IEEE, 2008, pp. 495–500.

[10] H. Ishii, Y. Wang, and S. Feng, "An overview on multi-agent consensus under adversarial attacks," *Annual Reviews in Control*, vol. 53, pp. 252–272, 2022.

[11] A. B. Alexandru, M. Morari, and G. J. Pappas, "Cloud-based mpc with encrypted data," in *2018 IEEE conference on decision and control (CDC)*. IEEE, 2018, pp. 5014–5019.

[12] F. Fotiadis and K. G. Vamvoudakis, "Concurrent receding horizon control and estimation against stealthy attacks," *IEEE Transactions on Automatic Control*, 2022.

[13] G. Marti, T. Kölle, and C. Studer, "Mitigating smart jammers in multi-user mimo," *IEEE Transactions on Signal Processing*, vol. 71, pp. 756–771, 2023.

[14] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410–1414, 2019.

[15] S. Vuppala, Y. J. Tolossa, G. Kaddoum, and G. Abreu, "On the physical layer security analysis of hybrid millimeter wave networks," *IEEE Transactions on Communications*, vol. 66, no. 3, pp. 1139–1152, 2017.

[16] S. Jajodia, A. Ghosh, V. Subrahmanian, V. Swarup, C. Wang, and X. Wang, *Moving Target Defense II: Application of Game Theory and Adversarial Modeling*, ser. Advances in Information Security. Springer New York, 2012. [Online]. Available: https://books.google.com/books?id=yFzKRGJatCIC

[17] V. Casola, A. De Benedictis, and M. Albanese, "A multi-layer moving target defense approach for protecting resource-constrained distributed devices," in *Integration of Reusable Systems*. Springer, 2014, pp. 299–324.

[18] J. H. Jafarian, E. Al-Shaer, and Q. Duan, "Openflow random host mutation: transparent moving target defense using software defined networking," in *Proceedings of the first workshop on Hot topics in software defined networks*. ACM, 2012, pp. 127–132.

[19] M. Dunlop, S. Groat, W. Urbanski, R. Marchany, and J. Tront, "Mt6d: A moving target ipv6 defense," in *Military Communications Conference, 2011-Milcom 2011*. IEEE, 2011, pp. 1321–1326.

[20] R. Zhuang, S. A. DeLoach, and X. Ou, "Towards a theory of moving target defense," in *Proceedings of the First ACM Workshop on Moving Target Defense*. ACM, 2014, pp. 31–40.

[21] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

[22] K. Shen and W. Yu, "Fractional programming for communication systems—part i: Power control and beamforming," *IEEE Transactions on Signal Processing*, vol. 66, no. 10, pp. 2616–2630, 2018.