IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 18, 2021, accepted March 5, 2021, date of publication March 10, 2021, date of current version March 19, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3065228

On the Use of Fibonacci Sequences for Detecting Injection Attacks in Cyber Physical Systems

SARA BALDONI[1], (Graduate Student Member, IEEE), FEDERICA BATTISTI[2], (Senior Member, IEEE), MARCO CARLI[1], (Senior Member, IEEE), AND FEDERICA PASCUCCI[1], (Member, IEEE)

[1]Department of Engineering, University of Roma Tre, 00146 Rome, Italy
[2]Department of Information Engineering, University of Padova, 35131 Padua, Italy

Corresponding author: Federica Battisti (federica.battisti@unipd.it)

This work was supported in part by the European Union's Horizon 2020 Research and Innovation Programme through the Project RESISTO under Grant 786409.

ABSTRACT Cyber Physical Systems are characterized by a strong interaction among networking, sensing, and control functionalities. Moreover, the recent advent of Internet of Things extended their information sharing capability. However, the interaction between Internet and Cyber Physical Systems requires increased efforts for guaranteeing the security of connected systems. In the industrial field, the problem becomes more complex due to the need of protecting a large attack surface while guaranteeing system availability and real-time response to the detection of threats. In this contribution, we deal with the injection of tampered data into the communication channel with the aim of modifying the status of the physical system. To cope with this attack, we design a secure control system able to detect the injection of tampered data by coding the output of the measurement systems. The proposed approach is based on the use of permutation matrices, whose scheme varies upon a secret pattern obtained exploiting the Fibonacci p-sequences. The detection strategy is compliant with the time delay constraints typical of a Cyber Physical System. An analysis of the security performances of the proposed system is presented along with the experimental proof of its effectiveness.

INDEX TERMS Cyber physical systems, Internet of Things, security, industrial control system, stealthy deception attacks.

I. INTRODUCTION

The fourth industrial revolution, namely Industry 4.0, introduces a new trend in automation: physical processes and decentralized controllers interact with humans to set up the smart factory. According to this new paradigm, the Cyber Physical Systems (CPS) evolved replacing the commonly used industrial networks with the Internet and exploiting the Internet of Things Services [1].

The Industrial Internet of Things (IIoT) requires the deployment of sensors, actuators, and communication devices in the physical infrastructures for allowing the remote monitoring and control of the whole system as well as of its components. The adoption of IIoT may allow a significant cost reduction by exploiting scale economies and in-deep process automation, and may be used to perform a step-by-step quality control thanks to the distributed deployment of the sensors. However, these improvements should also guarantee, and possibly enhance, the reliability, the robustness, and the security of the overall system [2]. In particular, security represents a fundamental challenge to cope with. IIoT is a distributed framework and for this reason it is prone to security issues that exponentially grow if even a small part of the communication infrastructure is based on Internet.

As for any communication infrastructure, security, confidentiality, and availability of the system should always be guaranteed. In particular, in IIoT CPS context, a key factor is the availability of the system and of the information that should be shared within real time delay constraints [3], [4]. Moreover, the reliability of the information is of primary importance: data alteration (due to communication errors or intentional manipulations) should be timely detected to grant fast and effective recovery actions.

Addressing these challenges and ensuring security in IIoT is a fundamental priority. Badly secured IIoT structures and services may be used as entry points for cyber attacks and

The associate editor coordinating the review of this manuscript and approving it for publication was Claudio Agostino Ardagna.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

expose both data and systems to threats. For this reason, this issue is largely discussed in the research community [5], [6]. In order to provide a secure and reliable IIoT environment, it is important to investigate possible attack surfaces on all abstraction layers, from the physical stack to the interaction with machine operators (as shown in Figure 1, [7]).

This work copes with threats that may arise in the communication channel. A survey about network attacks in CPS is presented in [8]. The key idea of the proposed method is to design a secure control system capable of detecting the injection of tampered data (known as deception attack). Specifically, we address the attacks highlighted in [9] that may not be detected until the physical system becomes unavailable. Our approach is based on coding the output of the system, as proposed in [10]–[12]. In more details, the measurements from sensors are coded by means of signed permutation matrices, whose scheme varies upon a secret sequence. The scheme has been introduced in [11] for linear systems, and applied to nonlinear systems in [12].

In this contribution we study the effectiveness of the method when considering a closed loop control system having exogenous inputs. Furthermore, the robustness of the approach is deeply investigated when the Fibonacci p-sequences, $F_p(n)$, are used to update of the coding matrix [13]. The introduction of the Fibonacci p-sequences allows to use a two-key-based encoding matrix selection since two parameters, p and n, have to be chosen. However, some issues are present. We highlight the weaknesses of the approach and propose procedures based on state-of-the-art for mitigating the security issues.

Our previous works, [11], [12], presented an innovation with respect to the approaches in [10], [14] in several aspects:

- with respect to [14], coding is adopted instead of encryption. This reduces the computational load of the security system: encryption, indeed, cannot be applied to real time and low energy consumption distributed systems [15]. Moreover, the coding allows to avoid the communication overhead typical of encryption algorithms [10];
- each coding matrix is obtained by rotating and flipping the identity matrix. This results in scrambling the elements of the output vector and in sign permutation. To the best of our knowledge, in literature only the rotation has been considered. In our model, the operation of flipping allows to enlarge the set of coding matrices thus resulting in an increased security;
- due to matrix multiplication, the encoding procedure might be affected by quantization errors that can be wrongly interpreted as an attack. In the proposed system this problem is not present due to the fact that the considered permutation matrices and their inverse are integer;
- the coding matrix is updated according to the Fibonacci p-sequences. One benefit in adopting these key-dependent sequences is an increase in the security level of the system. In fact, after the set of coding matrices has been defined, the current matrix index depends on the selected Fibonacci p-sequence. For this reason, the p value can be modified without affecting the computational complexity of the system;
- differently from [10], the coding matrix is updated at each transmission time. This operation decreases the probability of its disclosure;
- the use of the Fibonacci p-sequences allows to avoid synchronization problems by exploiting the communication protocol.

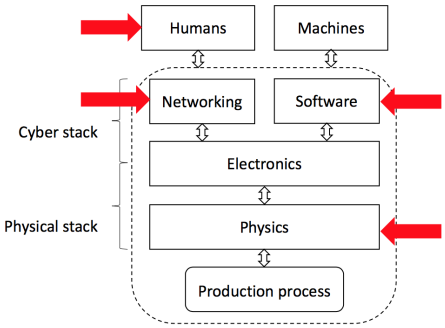


FIGURE 1. Components of IoT based CPS. The red arrows represent potential attack surfaces.

An in-depth analysis of the models introduced in [11], [12] highlighted some limitations. To cope with these issues, in this paper we introduce the following improvements:

- this paper presents a detailed security analysis. In more details, we investigate the use of non sequential values of n in the selection of the Fibonacci sequences. The n parameter is shared through a covert channel between the physical and the monitoring systems. Moreover, we address the security issues related to the use of a fixed p value, that may be solved by exploiting a refreshing key procedure;
- the experimental validation of the proposed approach is extended by including two real case scenarios (i.e., the pendubot and the self-balancing board).

The comparison with state-of-the-art approaches is summarized in Table 1.

The rest of the paper is organized as follows: Section II presents the state-of-the-art while in Section III the system model and the theoretical background are introduced. Section IV describes the detection strategy based on coding scheme, Section V includes the security analysis, and Section VI proposes the solution to the highlighted security issues. Then, Section VII reports the validation tests that have been performed to prove the effectiveness of the proposed method. Finally, in Section IX the conclusions are drawn.

II. RELATED WORKS

Connected CPS are characterized by a complex structure that may be prone to attacks in different points, thus resulting in a large attack surface [16]. Potential attacks can target three abstraction layers [17], as shown in Figure 1:

1) Human layer: people involved in the CPS project, management, or operators may be subject to social

TABLE 1. Comparison between the proposed method and state-of-the-art approaches.

Reference	Approach	Main drawbacks solved in the proposed approach
[14]	Encryption	Computational load higher than coding; Encryption communication overhead.
[10]	Coding matrices: float, obtained though rotations. Matrix update: heuristic algorithm for update time interval. Matrix selection: Givens rotation.	Quantization errors are possible; The matrix update time depends on an heuristic algorithm.
[11]	Coding matrices: integer, obtained through rotation and flipping. Matrix update: each time instant. Matrix selection: random.	No security key is present except from the random generator seed.
[12]	Coding matrices: integer, obtained through rotation and flipping. Matrix update: each time instant. Matrix selection: Fibonacci p-sequences, in sequential order, with fixed p.	Use of the sequential matrix selection with fixed p parameter.
Proposed	Coding matrices: integer, obtained through rotation and flipping. Matrix update: each time instant. Matrix selection: Fibonacci p-sequences, in non-sequential order, with varying p.	

engineering attacks exploiting *bugs* in human decision-making procedures;

2) Cyber layer encompasses different components:
   - *Communication*: networks are subject to many attacks, such as Denial of Service (DoS), Man in the Middle, injection attack, eavesdropping, etc. The impact of these attacks strictly depends on the specific CPS domain. As stated in the previous section, in many CPS application scenarios the injection attack can result in the fault of the complete system;
   - *Hardware*: microcontrollers, actuators, sensors, CPU, computers, storage devices can be subject to different attacks such as invasive hardware attack, reverse engineering, etc.;
   - *Software*: many attacks can be performed such as viruses, Trojans, and back doors.
3) Physical layer: attacks to the physical layer may affect both the electronics and the mechanics of the system [18].

In literature, the security assessment and the mitigation strategies in presence of attacks have been largely addressed for IIoT-based CPS. In particular, secure control theory is used for estimating the impact of cyber threats on the physical plant [19]. In [20] the attacks are classified on the basis of *model knowledge*, *disruption resources* and *disclosure resources*, that form the attack space. State-of-the-art methods are mostly devoted to deal with two types of menaces: Denial of Service (DoS) and deception-based attacks. One of the main threats of a DoS attack is that it is able to drive the system to an unsafe state [21]. A methodology for maximizing the effectiveness of a DoS attack on CPS in case of energy limitations is presented in [22]. In [23] the authors show that DoS, even if limited to a part of the network, may have a disruptive effect on the whole system. The proposed mitigation strategy is based on changing the routing topology for isolating the corrupted nodes. In addition, in [24], the dynamic output feedback method is used for addressing the presence of DoS.

In the deception-based attacks, the adversary gains access to the CPS first, and then injects malicious information towards or from sensors or controllers (e.g., the value of a measure, the sensor ID, or the updating command). An effective attack is designed to stay unnoticed to the detection system until a severe disruption occurs. As can be easily understood, while the implementation of a deception attack is more challenging for the attacker, its impact on the system may be disrupting. For this reason, in this work we deal with the detection of attacks belonging to this class. In [25] the design of stealthy deception attacks is proposed, while in [26] cases in which a stealthy deception attack may be performed without being detected are addressed. In [27], the authors show that resiliency to malicious data injection may be obtained if a subset of measurements is immune to attacks. However, selecting such subset is a high-complexity combinatorial problem given the typically large size of electrical grids. In [9], a false data injection attack model is presented as a constrained control problem. The theoretical analysis of the conditions under which the attacker could successfully destabilize the system is shown. An extended review of the security aspects is in [28]. The authors in [10] consider the presence of a smart attacker who can perform data injection in the system in such a way that the state estimation error increases without being detected till the moment when the effect of the attack is harmful for the system. The authors secure the system output by coding the sensor measurements through Givens rotation matrices. Similarly, encryption is exploited to protect data integrity and confidentiality in [14].

In this contribution we address the security issues presented in [10] and [14]. In more details, we modify the output coding scheme at each transmission time by selecting the coding matrix from a predefined set. The coding matrices are

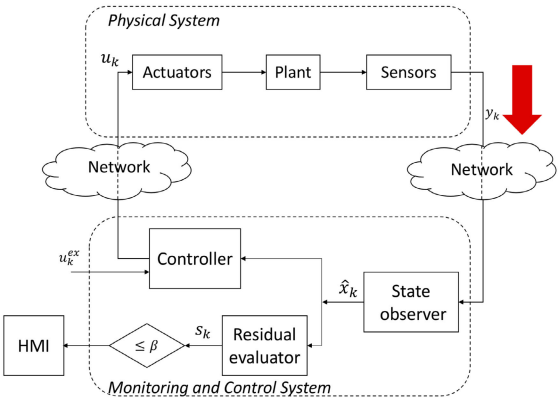


FIGURE 2. The industrial CPS and the detection scheme. The physical system is composed by actuators, plant, and sensors. The alarms are forwarded to the Human Machine Interface (HMI).

designed in order to avoid quantization errors and to reduce the computational complexity.

III. DEFINITIONS AND BACKGROUND

A. SYSTEM MODEL

The Industry 4.0 paradigm foresees the massive usage of communication in industrial control systems. To this aim, we consider the CPS described in Figure 2: its components (i.e., the *physical system* and the *monitoring and control system*) are connected to the network and, at each transmission time k, exchange sensors data and control signals.

In this work, we describe the *physical system* by a Linear Time-Invariant (LTI) uncertain system whose discrete time model is given by

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k + w_k \\ y_k &= Cx_k + v_k \end{aligned} \tag{1}$$

where $x_k \in \mathbb{R}^{n_x}$ are the state variables of the system, $u_k \in \mathbb{R}^{n_u}$ is the input, $y_k \in \mathbb{R}^{n_y}$ is the output, and $w_k \in \mathbb{R}^q$ and $v_k \in \mathbb{R}^l$ are the uncertainties that affect the process and the measurement, respectively. The noises w_k and v_k are modeled as zero-mean Gaussian stochastic variables, having known constant covariance matrices (i.e., $w_k \sim \mathcal{N}(0, Q)$ and $v_k \sim \mathcal{N}(0, R)$). The signal u_k is considered known and it is modeled as a deterministic variable.

The *monitoring and control system* can be further decomposed into three modules: the *state observer*, the *residual evaluator*, and the *controller*.

The *state observer*, given the input, the output, and the knowledge of the system, computes the state estimate $\hat{x}_k$ at each transmission time k. It is assumed that the physical system satisfies the constraints to set up a steady state Kalman filter, i.e. (C, A) is observable and (A, Q) is controllable, thus, the estimate is computed as:

$$\hat{x}_{k+1} = A\hat{x}_k + Bu_k + K[y_k - C(A\hat{x}_k + Bu_k)], \tag{2}$$

where K is the steady state Kalman gain

$$K \triangleq PC^T(CPC^T + R)^{-1}, \tag{3}$$

and P is the steady state error covariance matrix, retrieved as $P = APA^T + Q - APC^T(CPC^T + R)^{-1}CPA^T$. The state observer forwards the estimate to both the *residual evaluator* and the control system. The *residual evaluator* computes the residual as:

$$r_{k+1} = y_{k+1} - C(A\hat{x}_k + Bu_k), \tag{4}$$

where $r_k \sim \mathcal{N}(0, CP\,C^T + R)$ when the system is not under attack, and executes a χ^2–detector. More specifically, the weighted power of residual $s_k = r_k(CPC^T + R)^{-1}r_k^T$ is compared with a threshold β and the following decision rule $\mathscr{R}_k$ is applied

$$\mathscr{R}_k = \begin{cases} \mathscr{H}_0 & \text{if } s_k \leq \beta \\ \mathscr{H}_1 & \text{if } s_k > \beta \end{cases}$$

where $\mathscr{H}_0$ and $\mathscr{H}_1$ are the *healthy* and *under attack* hypothesis, respectively. An alarm is activated when the threshold is overtaken and the information is forwarded to the human machine interface.

The *controller* is implemented as a Linear Quadratic Gaussian (LQG), so the following quadratic cost function is considered

$$\mathscr{J}(x, u) = \lim_{k\to\infty} \sum_{j=0}^{k-1} \left(x_j^T W x_j + u_j^T U u_j\right)$$

where U and W are positive semidefinite matrices. Concerning regulation problems, i.e., $u_k^{ex} = 0, \forall k = 0, 1, \ldots$, the control law that minimizes $\mathscr{J}(\cdot)$ is $u_k = L\hat{x}_k$. The matrix L is obtained as

$$L = -(B^T SB + U)^{-1}B^T SA \tag{5}$$

where the matrix S satisfies the following Riccati equation $S = A^T SA + W - A^T SB(B^T SB + U)^{-1}B^T SA$. If the matrices $(A - KCA)$ and $(A + BL)$ are stable, the overall CPS is stable, i.e., at steady state the variables $\{x_k, y_k, \hat{x}_k\}$ represent stationary random processes. To track the general input u_k^{ex}, the feedforward approach can be adopted, so the control law that minimizes $\mathscr{J}(\cdot)$ is

$$u_k = L\hat{x}_k + L^{ex}u_k^{ex}, \tag{6}$$

where

$$L^{ex} = -[C(A - BK)^{-1}B]^{-1}. \tag{7}$$

It is worth noticing that a solution for the tracking problem cannot always be retrieved, since it depends on the input and output vector dimension.

B. ADVERSARY MODEL

In this work, the adversary is assumed to be able to gain the control of the measurement communication channel, potentially bypassing the attack detection tool such as an intrusion detection system. The adversary objective is to drive the system to an unsafe state while remaining stealthy.

According to the envisioned CPS, the stealthy constraint is satisfied by modifying the sensor measure without affecting the statistical properties of $\hat{x}_k$, y_k, and r_k. In this way, the weighted power of the residual s_k is bounded, and the χ^2–detector cannot distinguish the $\mathscr{H}_0$ *healthy* hypothesis from the harmed system. To achieve the goal, the attack should drive the error $e_k \triangleq x_k - \hat{x}_k$ to grow unbounded, i.e. $\lim_{k\to\infty} \|e_k\| = \infty$. It is worth noticing that the goal of the attack is to reduce the resource availability; however, it is achieved by compromising data integrity due to the stealthy constraint.

The attack policy a_k, indeed, modifies sensor measurements y_k from their expected value

$$\tilde{y}_k = y_k + a_k = y_k + \Gamma y_k^a \tag{8}$$

where $y_k^a \in \mathbb{R}^{n_a}$ represents the data corruption and $\Gamma \in \mathbb{B}^{n_y \times n_a}$ ($\mathbb{B} \triangleq \{0, 1\}$) is the binary incidence matrix mapping data corruption to the corresponding measurement.

According to [20], the *model knowledge* and the *disruption resources* of the adversary encompass both the plant and the monitoring systems, while no *disclosure resources* are exploited during the attack.

As shown in [9], the success of the attack depends on:

- the possibility of harming the system: the matrix A should have at least one unstable eigenvalue;
- the possibility of controlling the error dynamics e_k: the eigenvector ξ, corresponding to the unstable eigenvalue, should lie in the reachable subspace associated to the pair $(A - KCA, K\Gamma)$, i.e. $\xi \in \text{span}\{O_{K\Gamma}\}$, where $O_{K\Gamma}$ is the correspondent controllability matrix;
- the possibility of affecting the error e_k by corrupting only a subset of sensors: the eigenvector ξ filtered by the measurements lies in the subspace of the attacked sensors, i.e., $C\xi \in \text{span}\{\Gamma\}$.

IV. DETECTION STRATEGY

To detect a deception attack on the sensors data, a simple protection for the communication channel is considered. As highlighted in [10], the security scheme should not affect the real time constraints of the industrial control system and, at the same time, it should be able to change the statistical properties of the residual. In [10], the authors introduce a security scheme based on coding the output by pre-multiplying it for a suitable matrix Φ. The coding matrix is able to change the statistical properties of the residual provided that the direction of the vector $\Phi C\xi$ is different from the one of $C\xi$. In [11], the result is further improved by considering a set of coding matrices $\mathscr{S}_\Phi \triangleq \{\Phi_i | \exists \Phi_i^{-1} \forall i \in 1, 2, \ldots, m\}$ that change at each transmission time according to a secret predefined pattern.

Here, we adopt a similar approach, considering the set of the *signed permutation matrices* $\mathscr{S}_\Pi$. A signed permutation matrix shows the following property: it has exactly one non-zero entry (either 1 or -1) in each row/column. Coding the output using a signed permutation matrix results in flipping and rotating the output vector, allowing the change of the statistical properties of the residual, as detailed below. Moreover, the set of the signed permutation matrices forms a group with integer inverse, thus the encoding procedure does not introduce quantization errors and satisfies the real time constraint. The computation of the set $\mathscr{S}_\Pi$ is a combinatorial problem, since the cardinality of the set $\mathscr{S}_\Pi$ depends on the number of system outputs n_y according to the following relation:

$$|\mathscr{S}_\Pi| = n_y! 2^{n_y}. \tag{9}$$

Given a $n_y \times n_y$ matrix, indeed, the number of unsigned permutations is $n_y!$. Moreover, since each matrix has exactly one non-zero entry in each row and column, the number of sign combinations is equal to the combination of n_y bits. It is worth noticing, however, that the generation of the set $\mathscr{S}_\Pi$ is performed once and off-line. The computational complexity can be further reduced by exploiting some properties (e.g., symmetry and orthogonality) of the hyper-octahedral groups. Moreover, as shown in [11], only a subset of the set $\mathscr{S}_\Pi$ can be effectively used for coding. Specifically, as proposed in [11], the *set of feasible matrices* $\mathscr{S}_\Phi \subset \mathscr{S}_\Pi$ is retrieved by applying the following test to each element $\Pi_i \in \mathscr{S}_\Pi$:

$$\frac{|(C\xi)^T \Pi_i C\xi|}{\|\Pi_i C\xi\|_2 \|C\xi\|_2} \neq 1.$$

To modify the coding matrix at each transmission time, a secret pattern needs to be shared between the plant and the control and monitoring system. In this work, we propose to sort the set of feasible matrices $\mathscr{S}_\Phi$ and choose the coding matrix in the sorted set using the Fibonacci p-sequences. A Fibonacci p-sequence $F_p(n)$ is defined by the following recursive formula:

$$F_p(n) = \begin{cases} 0, & n < 0; \\ 1, & n = 0; \\ F_p(n-1) + F_p(n-p-1), & \textit{otherwise}. \end{cases} \tag{10}$$

Different values of p define different p-sequences. Since the number of feasible rotation and flipping operations performed for obtaining the coded output is limited to $|\mathscr{S}_\Phi| = m$, there is the need for mapping the selected Fibonacci p-sequence to the interval $[0, \ldots, m-1]$ by means of modulo-m operations. As for the computational cost, it is worth mentioning that the matrix selection based on $F_p(n)$ requires only the computation of sums, and the coding procedure is equivalent to a single multiplication. Moreover, aiming at analyzing the limitations of the approaches presented in [11], [12], in the following we consider the case in which the n parameter is represented by the sequence number of the packet in the data stream.

V. SECURITY ISSUES

To better clarify the security challenges introduced by [11], [12], in the following the main building blocks of the proposed method are detailed.

The system can be completely described by: the system parameters, $\{A, B, C, Q, R, L, L^{ex}, K\}$, the output signal, y, and the input signal, u.

The protection system is characterized by three security levels:

- the set of the feasible matrices $\mathscr{S}_\Phi$;
- the sorting of the feasible matrix set $\mathscr{S}_\Phi$;
- the matrix selection procedure: in our case the Fibonacci sequence parameters p and n.

To analyze the robustness of the proposed approach, let us consider a smart adversary who knows the system parameters, eavesdrops both y and u channels, and knows which kind of encoding sequence has been applied. Moreover, knowing the number of system outputs and the results on which the coding scheme is based, he/she is able to infer the set of feasible coding matrices. In addition, let us assume that, after each transmission the attacker is able to retrieve the employed coding matrix. This knowledge can be obtained as described in the following. By eavesdropping the coded measurement y_k, and knowing all the possible coding matrices, the attacker can generate a set of candidate decoded measurements, $\{y_k^C\}$. In addition, the attacker needs $\hat{x}_{k-1}$ to compute $\hat{x}_k$ and thus a set of candidate system inputs, $\{u_k^C\}$. By eavesdropping the transmitted u_k, and comparing it to the set $\{u_k^C\}$ he/she is able to retrieve the employed coding matrix. It is useful to notice that $\hat{x}_{k-1}$ can be obtained at least in three ways. As first possibility, if the matrix L has full column rank, it can be retrieved by inverting Equation 6. As second option, it can be computed by simulating the behavior of the system from the first time instant knowing the initial state. At last, it can be accessed by corrupting the *state observer*. Let us highlight that these strong assumptions are exploited to analyze the security issues of the approach presented in [11], [12] in the most challenging scenario.

Under these hypotheses, the adversary is missing only three elements: the sorting of the feasible matrix set $\mathscr{S}_\Phi$ and the Fibonacci parameters p and n. These parameters can be regarded as three independent random variables. To evaluate the robustness of the proposed approach we consider as key performance indicator the time needed by the adversary to gain knowledge about a parameter, TI, given that two out of three parameters are known. According to this methodology, three cases can occur:

(a) the adversary knows p and n;
(b) the adversary knows the matrix set sorting and p;
(c) the adversary knows the matrix set sorting and n.

Case (a): let us consider the best situation for the adversary, namely the case in which all the possible matrices are chosen without repetitions (see, for example, Fig. 3 from time instant 44 to 88). After computing the position of the first matrix, then, he/she has to arrange $m-2$ matrices to obtain the adopted order. In other words, it takes $TI = m-1$ time instants to obtain the desired information.

Case (b): we suppose that n increases sequentially (i.e., $n = 0, 1, \dots$). Since the adversary knows p, he/she is able to compute the entire Fibonacci p-sequence, $F_p(n)$ mod m. Moreover, since the sorting of the feasible matrix is known, after eavesdropping the output data in a certain time interval T, he/she can also compute $F_p^a(n)$, that is the sub-sequence used to code the output during the time interval T. Thus, the key performance indicator is the length of this time interval: when $F_p^a(n)$ is unique in $F_p(n)$, the adversary can infer the n parameter and predict the future coding matrices. It should be noticed that, as demonstrated in [29], the sequence $F_p(n)$ mod m forms a periodic series: the length of the time interval T is related to this period. In the worst case $TI = \text{length}(T) = 2$ time instants.

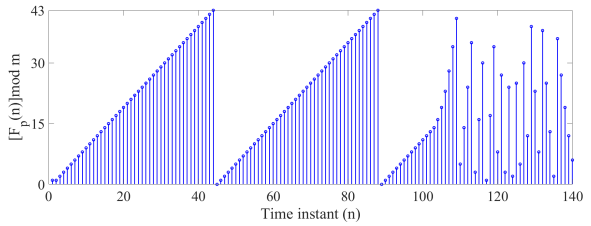


FIGURE 3. The Fibonacci 100-sequence, for $m = 44$.

Case (c): the adversary does not know the parameter p. However we may suppose that $p \in P = \{p_i, \dots, p_f\}$ and P is known by the adversary once the security protocol is made public. The adversary can compute offline the sequences $F_p(n)$ mod m for the different values of the parameter $p \in P$. Knowing n, he/she can also define at each instant of time k a subset of sequences $F_k = \{F_{p_1}^a(n) \bmod m, \dots, F_{p_d}^a(n) \bmod m\}$, that assumes the same value for n at time k. Defining

$$\mathscr{F} = \bigcap_{k=1,\dots,h} F_k,$$

the key performance indicator is represented by the minimum time h the adversary needs to reduce this set to a single sequence, namely $|\mathscr{F}| = 1$. This performance index can be computed considering the Fibonacci sequence generation process. As shown in Equation 10, the first p elements of the sequence are obtained as sum of 1 and 0, thus providing $F_p(n) = 1$. It is possible to eliminate the first p elements from the output sequence, by using the Fibonacci sequence starting from $n = p$. This corresponds to set the sequence origin in $n = p$. The new sequence, following Equation 10, will be:

$$F_p(n) = \begin{cases} 0, & n < -p \\ 1, & -p \le n \le 1; \\ F_p(n-1) + F_p(n-p-1), & otherwise. \end{cases} \quad (11)$$

Anyway, as shown in Equation 11, the presence of long runs of 1 and 0 still affects the computation of the elements in the sequence for $n > 1$. The result is a ramp function from 0 to $m-1$. The ramp repeats until $F_p(n-p-1)$ belongs to the run of ones. Due to this feature, all sequences start the same way thus making more difficult the identification of the p parameter. However, by observing the ramp, the attacker

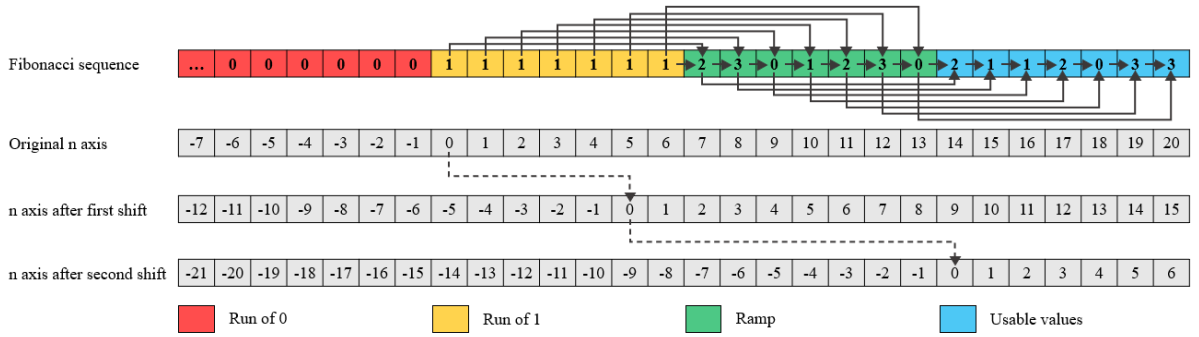


FIGURE 4. Origin shift procedure for $p = 6$ and $m = 4$. The solid arrows indicate the $F_p(n)$ computation, whereas the dashed arrows represent the origin shifts.

can predict the used matrices and can easily compute the p value when the ramp stops.

As shown by Equation 11, after the sequence origin shift, $F_p(0) = 1$ and $F_p(1) = 1$. As a consequence, in order to avoid the ramp, we need to set:

$$n - p - 1 \geq 2$$

hence

$$n \geq p + 3.$$

Equation 11 can then be rewritten as:

$$F_p(n) = \begin{cases} 0, & n < -p \\ 1, & -p \leq n \leq 1; \\ ramp\{0; m-1\}, & 1 < n < p+3 \\ F_p(n-1) + F_p(n-p-1), & otherwise. \end{cases} \tag{12}$$

A possible solution might be shifting the sequence origin for all p values, and consequently removing the ramp. Unfortunately, this approach introduces new issues. Let us set the sequence origin in $p + 3$, thus defining the new sequence:

$$F_p(n) = \begin{cases} 0, & n < -2p-3 \\ 1, & -2p-3 \leq n \leq \\ & -p-2; \\ ramp\{0; m-1\}, & -p-2 < n < 0 \\ F_p(n-1) + F_p(n-p-1), & otherwise. \end{cases} \tag{13}$$

An example of the origin shift procedure is summarized in Figure 4 for $p = 6$ and $m = 4$.

It is useful to notice that for consecutive values of p, the n value for which the ramp stops is consecutive too, so that the origin shift is different for every p. Moreover, following Equation 13, even using $F_p(n)$ for $n \geq 0$, the elements of the ramp are still used for the computation of the sequence until when $F_p(n - p - 1)$ belongs to the ramp. Due to these phenomena, a new $F_p(n)$ ramp arises. In more details, for the same n, all $F_p(n)$ take a value in the range $[0, m - 1]$ following an increasing trend. This effect is shown in Table 2 for $m = 44$. The p-ramp continues until when $F_p(n - p - 1)$ belongs to the n-ramp. Exploiting Equation 13, this happens when:

$$n - p - 1 \geq 0$$

hence

$$n \geq p + 1.$$

As can be noticed, the length of the ramp depends on the magnitude of p (i.e. a smaller p entails a shorter ramp).

From this analysis, we can infer that if we consider a p range smaller than m, the attacker will take a single time instant to find out p. If the p range is larger, we have a group of sequences which are equal until one of them stops being part of the p-ramp, namely when $n = p + 1$. Considering the worst case and setting $p = 1$, we obtain $TI = 2$ time instants.

TABLE 2. Fibonacci sequences: p-ramp table. For every n, a vertical ramp is present.

p \ n	0	1	2	3	4	5	6	7	8	9	10
1	5	8	13	21	34	11	1	12	13	25	38
2	6	9	13	19	28	41	16	0	41	13	13
3	7	10	14	19	26	36	6	25	7	43	5
4	8	11	15	20	26	34	1	16	36	18	8
5	9	12	16	21	27	34	43	11	27	4	31
6	10	13	17	22	28	35	43	9	22	39	17
7	11	14	18	23	29	36	0	9	20	34	8
8	12	15	19	24	30	37	1	10	20	32	3
9	13	16	20	25	31	38	2	11	21	32	1
10	14	17	21	26	32	39	3	12	22	33	1

VI. SECURITY SOLUTIONS

The analysis of the key performance indicator highlighted some security issues in the three cases considered in Section V. These issues are related to:

- the sequential trend of n (i.e., the number of the packet in the communication sequence);
- the fixed parameter p.

Case (a) can be avoided by varying n in a non-sequential order. Moreover, when n has a non monotonous trend, the p-ramp problem does not exist and, consequently, case (b) is prevented. It is worth to notice that, whereas using a sequential n implies that the adversary must know one value of

n to compute the others, if it varies in a different way he/she should perform the procedure for discovering n at each iteration.

To cope with the security issues related to the adoption of a fixed value for the parameter p, we propose to change its value periodically. Even assuming that the attacker is able to obtain n and p, he needs $m-1$ time instants more to gain the complete knowledge. Changing p each $m-1$ instants, for example, could avoid this possibility. Moreover, by changing the p parameter, the issue related to the period of the sequence $F_p(\text{mod } m)$ is prevented.

To implement these improvements, a secure way for transmitting n and p is needed. As detailed in the following, for the first parameter a covert channel is adopted while for the second one a refreshing key procedure is used.

A. SHARING THE n PARAMETER

A covert channel is defined as *any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy* [30]. Typically, it is possible to distinguish between timing and storage channels. The former aims at modifying a timing attribute (e.g. the inter-packet arrival delay) to transmit a covert message. The storage channels, on the contrary, make use of reserved or unused fields of packet headers to write covert messages. As suggested in [31] and [32], this well-known malicious technique can be used to protect network transmissions. In [31], for instance, the Modbus Covert Channel Integrity Check is proposed to provide private communications outside the purview of the attacker. In [32], the use of covert channel for authentication purposes can be found. Moreover, the authors highlight that one of the key benefits of using covert channels is that they do not introduce protocol modifications or traffic overheads. As a consequence, the cost of sharing the n parameter through covert channel can be considered smaller than the one needed for encryption.

The choice of the specific covert channel methodology to be adopted is beyond the scope of this work. In the performed test, we assume that a covert channel exist and that the n values are correctly available at the monitoring and control system. Moreover, let us note that in our model the capacity of the covert channel is limited and therefore not suitable for the transmission of the sensors measurements.

B. SHARING THE p PARAMETER

A possible solution to synchronize the value of p in the physical system and in the monitoring and control system is to exploit a key exchange procedure.

Based on the work presented in [33], we argue that an Authenticated Key Agreement (AKA) protocol can be used. In these protocols, private and ephemeral secret keys are used to produce a common session key between the parties while authenticating each other. In our case, rather than computing an encryption session key, the p parameter is obtained. To this aim, a suitable approach is defined in [33], where the authors propose a leakage resilient AKA (LR-AKA) robust to side-channel attacks. A side-channel attack is defined as an attack in which the adversary can obtain fractional information about the private/ephemeral keys while users execute the cryptographic protocols. LR-AKA should tolerate the fractional leakage of keys while ensuring security. To do this, a possible solution is to split the private key into two components and update them after each session key generation procedure. Initially, the private and public keys of each party are generated. Then, the session key generation procedure starts. This second phase is further split in two steps: key refreshing and key agreement. During key refreshing private keys are updated. During key agreement, the two parties compute independently the same session key. In the same way, the physical system and the monitoring and control system can update periodically their private keys and generate a new p parameter. Let us note that, differently from a cryptographic key which is usually longer than 128 bits, the p parameter requires a limited number of bits (e.g. 10). Moreover, independently from the adopted cryptographic primitive, if the attacker is able to break it when encryption is used, the whole security system will be destroyed. On the contrary, our choice of using a two-parameter coding scheme makes our security system robust with respect to such issue.

VII. VALIDATION

The proposed approach is validated by simulating two systems: a pendubot and a self-balancing board. In both experiments, we consider that sensors and actuators are linked to the monitoring and control system by a communication channel. This channel is penetrated by the adversary that sets up a stealth attack. In the following, we show that the proposed coding scheme succeeds in detecting the attack.

A. ATTACK TO PENDUBOT

In the first experiment the system considered is a pendubot, i.e., a vertical two-link planar robot (see [34] for further details): it is an under-actuated manipulator, since it has two links and only one actuator. The state variables represent the angles (rad) and the angular velocities (rad/s) of the joints, while the control is the torque on the first link. The system is usually described by a non-linear model. However, when stabilized in the unstable equilibrium point, a linearized model can be used. We consider the system proposed in [34], described by the following matrices:

$$A = \begin{bmatrix} 1.001 & 0.005 & 0.000 & 0.000 \\ 0.350 & 1.001 & -0.135 & 0.000 \\ -0.001 & 0.000 & 1.001 & 0.005 \\ -0.375 & -0.001 & 0.590 & 1.001 \end{bmatrix}$$

$$B = \begin{bmatrix} 0.001 \\ 0.540 \\ -0.002 \\ -1.066 \end{bmatrix} \quad C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

The uncertainty affecting the system and the observation model is represented by the covariance matrices

$$Q = q \cdot q^T \quad R = 0.5 \cdot \mathbf{I}_{2\times 2}$$

where $q = [0.003 \;\; 1.000 \;\; -0.005 \;\; -2.150]^T$. We consider a regulation problem, so the objective of the LQG controller is to maintain the robot in the unstable equilibrium point. The weights of the controller are

$$W = \text{diag}\{5 \;\; 1 \;\; 1 \;\; 1\} \;\text{ and }\; U = 2,$$

respectively.

The residual generator is a steady state Kalman filter with

$$K = \begin{bmatrix} 0.0846 & -0.0479 \\ 1.0261 & -1.2301 \\ -0.0479 & 0.1610 \\ -1.4098 & 3.1248 \end{bmatrix}$$

and gains of the LQG controller are $L^e x = 0$ and

$$L = -\begin{bmatrix} 17.2460 & 3.1429 & 17.3186 & 2.1740 \end{bmatrix}.$$

The attack sequence is $a_k = \Gamma y_k^a$, where $\Gamma = \mathbf{I}_{2\times 2}$ and

$$\begin{aligned} y_0^a &= [0.6386 \;\; -0.7695]^T \\ y_1^a &= [-0.2267 \;\; 0.6639]^T \\ y_2^a &= [-0.4620 \;\; 0.7891]^T \\ y_3^a &= [0.0999 \;\; -0.7481]^T \\ y_k^a &= y_{k-4}^a - 1.06^{(k-4)} * [-0.0019 \;\; 0.0055]^T \\ \forall k &= 4, 5, \ldots \end{aligned}$$

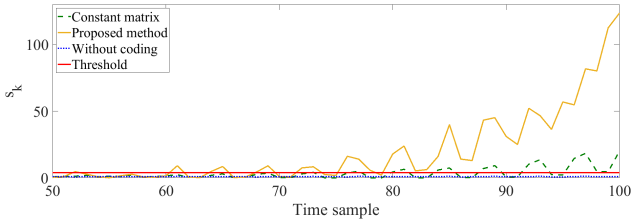
according to the constructive proof presented in [9]. The cardinality of the feasible coding matrices is $|\mathscr{S}_\Phi| = 6$, and

$$\mathscr{S}_\Phi = \left\{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \right\}.$$

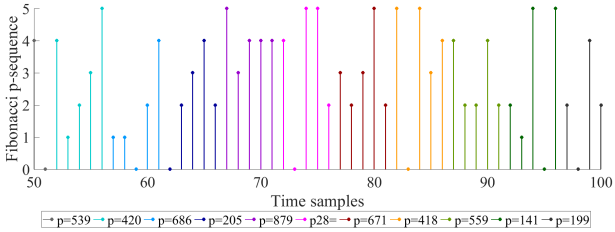
The obtained results are reported in Figure 5. In Figure 5(a), the signal s_k retrieved using the proposed technique is reported and compared with the ones computed without coding and using a fixed coding matrix $\Phi_i \in \mathscr{S}_\Phi$. To show the fixed coding matrix performances, among the feasible signed permutation matrices, we selected the one which allows to detect the attack earlier. As can be noticed, the use of the proposed method outperforms the others, allowing for faster and more reliable detection. In Figure 5(b), the coding sequence is reported using

$$\begin{aligned} p = [\; &418 \; 721 \;\; 1 \;\; 303 \; 147 \;\; 93 \; 187 \; 346 \; 397 \; 539 \\ &\times \; 420 \; 686 \; 205 \; 879 \;\; 28 \; 671 \; 418 \; 559 \; 141 \; 199 \;]. \end{aligned}$$

The p parameter has been updated every 5 instants, being the number of feasible matrices equal to 6. The p values have been generated as uniformly distributed pseudorandom integers in the range $[1, \ldots, 1000]$. Moreover, for each time instant, the n value has been generated as a uniformly distributed pseudorandom integer too. In this way we tried to mimic the parameter exchange process.



(a) Evolution of the weighted norm s_k over time: the blue dotted line is the signal without encoding, the green dashed line is obtained using a fixed encoding matrix, the solid yellow line is the result of the proposed method and the solid red line is the threshold



(b) Corresponding Fibonacci-generated sequence. Different colors represent different values of the p parameter

FIGURE 5. **Results of the experiment using the system proposed in [34].**

B. SELF-BALANCING BOARD

In the second experiment, the system represents a self-balancing unicycle robot moving on a straight line at constant speed. The state variables represent the driving speed, the pitch angle, and the pitch rate (see [35] for further details). The model of the system is nonlinear; however we consider, as in [35], the initial condition $X_0 = \begin{bmatrix} 0 \; 1 \; 0 \end{bmatrix}^T$, which means that the initial pitch angle is 1 rad, the driving speed is 0 m/s, and the pitch angular velocity is 0 rad/s, and linearize accordingly the model. The discrete time system is described by the following matrices:

$$A = \begin{bmatrix} 0.9684 & -0.0044 & 0 \\ 0.0001 & 1 & 0.0008 \\ 0.1815 & 0.0758 & 1 \end{bmatrix}$$

$$B = \begin{bmatrix} 0.0029 & 0 & -0.0142 \end{bmatrix}^T \quad C = \mathbf{I}_{3\times 3}.$$

The uncertainty that affects the system and the observation model is represented by the covariance matrices

$$Q = 0.5 \times \mathbf{I}_{3\times 3} \text{ and } R = \mathbf{I}_{3\times 3}.$$

The weights of the LQG controller are

$$W = \text{diag}\{100 \;\; 100 \;\; 50\} \text{ and } U = 1,$$

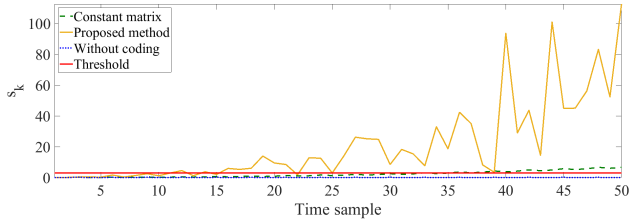
respectively.

The residual generator is a steady state Kalman filter with

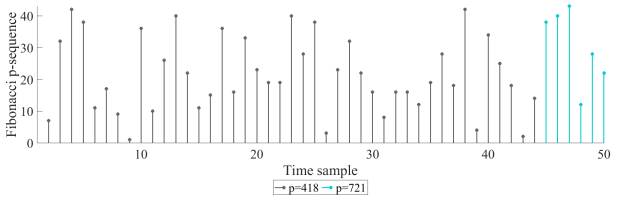
$$K = \begin{bmatrix} 0.4874 & -0.0017 & 0.0284 \\ -0.0017 & 0.4996 & 0.0125 \\ 0.0284 & 0.0125 & 0.5076 \end{bmatrix}.$$

The objective of the control is to drive the self balancing board along a line at constant speed ($1\,m/s$), so $u^e x_k = \begin{bmatrix} 1 \; 0 \; 0 \end{bmatrix}^T$. The gain L of the LQG controller is

$$L = \begin{bmatrix} -163.7452 & -311.9358 & -38.4794 \end{bmatrix}.$$



(a) Evolution of the weighted norm s_k over time: the blue dotted line is the signal without encoding, the green dashed line is obtained using a fixed encoding matrix, the solid yellow line is the result of the proposed method, and the solid red line is the threshold



(b) Corresponding Fibonacci-generated sequence. Different colors represent different values of the p parameter

FIGURE 6. Results of the experiment using the system proposed in [35].

and the gain $L^e x$ is computed as $L^{ex} = -[C(A-BK)^{-1}B]^{\dagger} = \begin{bmatrix}0.003217 & 0.0000064 & -0.016124\end{bmatrix}^T$ where the operator $\dagger$ represents the left pseudoinverse matrix operator.

The attack sequence is $a_k = \Gamma y_k^a$, where

$$\Gamma = \mathbf{I}_{3\times 3}$$
$$y_0^a = [0.0550 \;\; 0.0692 \;\; 0.3636]^T$$
$$y_1^a = [0.0236 \;\; 0.1031 \;\; 0.7335]^T$$
$$y_2^a = [-0.1309 \;\; 0.1333 \;\; 1.4669]^T$$
$$y_k^a = y_{k-3}^a - 1.0066^{(k-3)}[0.0138 \;\; -0.1183 \;\; -0.9785]^T$$
$$\forall k == 3, 4, \ldots$$

The cardinality of the feasible coding matrices is $|\mathscr{S}_\Phi| = 44$.

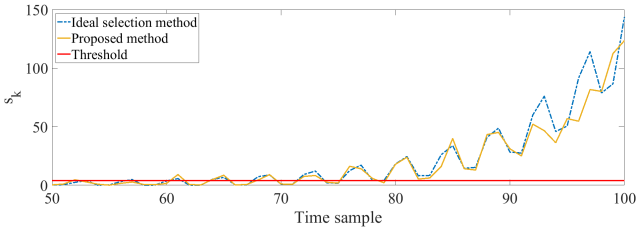
The obtained results are reported in Figure 6: the trend of s_k over the time is shown in Figure 6(a), when the shared key vector $p = [\;418 \;\; 721 \;\; 1\;]$ generates the sequence in Figure 6(b). The p parameter has been updated every 43 instants, being the number of feasible matrices equal to 44. The p values have been generated as uniformly distributed pseudorandom integers in the range $[1, \cdots, 1000]$. Moreover, for each time instant the n value has been generated as a uniformly distributed pseudorandom integer. In this way we tried to mimic the parameter exchange process. In the same figure, the trend of s_k without coding and using a fixed coding matrix $\Phi_i \in \mathscr{S}_\Phi$ is reported.

VIII. DISCUSSION

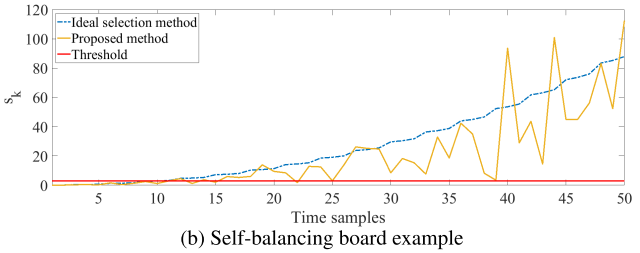
In order to assess the performances of the proposed method, we compared our results to the ones obtained when a constant coding matrix is used. As shown in Figures 5(a) and 6(a), the proposed matrix selection technique significantly outperforms the constant matrix approach. In fact, s_k grows rapidly thus enabling a faster attack detection. To further highlight the obtained improvement, we selected two key parameters: the first time sample for which s_k is greater than the threshold (T_{first}), and the time sample from which it remains permanently above the threshold ($T_{permanent}$). The comparison between the two methods is shown in Table 3.

TABLE 3. Comparison between the proposed method, the constant matrix selection technique and the ideal coding scheme.

Example	Method	T_{first}	$T_{permanent}$
Pendubot	**Proposed**	**52**	**80**
	Constant	73	96
	Ideal	53	76
Self-balancing Board	**Proposed**	**12**	**26**
	Constant	33	36
	Ideal	11	11



(a) Pendubot example

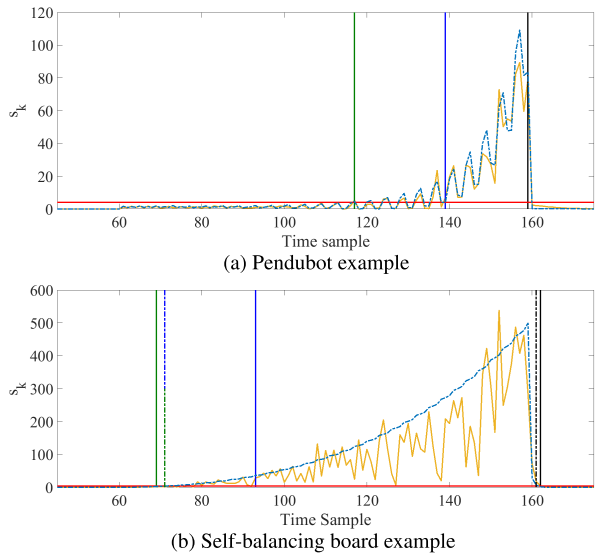


(b) Self-balancing board example

FIGURE 7. Evolution of the weighted norm s_k over time: comparison between the proposed method and the ideal matrix selection procedure.

Furthermore, we compared our results with those obtained with the ideal coding scheme. Specifically, for each time instant, the ideal matrix is the one that maximises the value of s_k. Let us note that, since the selection depends on the attack value, the ideal coding scheme cannot be implemented in practice. The trend of s_k under the ideal selection method, however, can be exploited to show how effective the proposed matrix selection procedure is. The comparison between the proposed approach and the ideal coding scheme is shown in Figure 7. As can be noticed, the trend of s_k when the proposed approach is employed (represented by the yellow solid line) is very close to the one achieved with the ideal selection method (represented by the blue dashed line). Moreover, for both examples, T_{first} and $T_{permantent}$ are close enough to the ideal case, as shown in Table 3.

Additionally, we tested our coding method in presence of a delayed and non-persistent attack. In more details, we have considered an attack starting at $t = 60$ and ending at $t = 160$. The behaviour of s_k both for the proposed and the ideal method is shown in Figure 8. The result for the proposed



(a) Pendubot example

(b) Self-balancing board example

FIGURE 8. Evolution of the weighted norm s_k over time: comparison between the proposed method and the ideal matrix selection procedure for a non persistent attack. The yellow solid line represents the proposed method performances, the blue dashed line represents the ideal scheme performances, and the red solid line represents the threshold. In addition, the green solid and dashed vertical lines represent T_{first} for the proposed and ideal method, respectively. The blue solid and dashed vertical lines represent $T_{persistent}$ for the proposed and ideal method, respectively. The black solid and dashed vertical lines represent T_{end} for the proposed and ideal method, respectively.

technique is represented by the solid yellow line, whereas the blue dashed line shows the ideal method behaviour. In addition, the first solid and dashed vertical lines represent T_{first} for the proposed and the ideal method, respectively. Similarly, the second solid and dashed lines represent $T_{persistent}$ which, for the non-persistent attack, is the time instant from which s_k remains above the threshold until the end of the attack. Finally, the third solid and dashed lines represent the time instant, T_{end}, for which s_k becomes smaller than the threshold after the end of the attack. From Figure 8 several considerations arise. First of all, let us note that the detection delay under a non-persistent attack is almost the same experienced for the persistent one. Also, for the pendubot, T_{first}, $T_{persistent}$, and T_{end} are the same for the ideal and the proposed methods. For the self-balancing board, however, the proposed approach is able to obtain a value T_{first} smaller than the ideal one. We note that this phenomenon is possible since the value assumed by s_k, and therefore the ideal coding matrix, depends on the past history of the system. In fact, the use of a different sequence of matrices leads to different system histories. Concerning $T_{persistent}$, as shown in the figure, for the ideal scheme it is equal to T_{first}. As for the proposed method, on the contrary, it is higher. This behaviour is due to the oscillations experienced by s_k due to the Fibonacci matrix selection procedure. In the end, T_{end} is almost the same for both methods. The performed comparisons clearly show the improvements obtained over the constant matrix approach, as well as the proximity to the ideal coding scheme.

Finally, let us highlight that the tests and considerations performed are not limited to the Fibonacci p-numbers. Such sequences, in fact, belong to the broader family of recurrent sequences. An example is represented by Lucas p-numbers which differ from Fibonacci's only for the initial conditions. The achieved results, as a consequence, are not limited to the Fibonacci p-numbers but, on the contrary, are valid for a wide range of sequences which could be used for the coding matrix selection.

IX. CONCLUSION

In this contribution, a method for securing IoT based CPS through the timely detection of deception attacks is presented. The proposed approach is based on coding the output of the system by using signed permutation matrices which result in flipping and rotating the output vector. The selection of the specific permutation matrix is based on Fibonacci p-sequences resulting in a two-keys security system. The proposed detection strategy is compliant with the time delay constraints typical of CPS. Furthermore, quantization errors, that may have a nonlinear behavior and can compromise the convergence of the residual estimator, are avoided. The performed tests demonstrate the effectiveness of the proposed approach. Concerning the challenges that may be addressed by future research, let us mention the implementation of the covert channel for transmitting the n parameter, and the exploitation of the properties of the hyper-octahedral groups (e.g., symmetry and orthogonality) for reducing the offline computational complexity. In addition, the implementation of a real test-bed will allow the validation of the proposed approach using industrial communication protocols.

REFERENCES

[1] B. Dorsemaine, J. P. Gaulier, J. P. Wary, N. Kheir, and P. Urien, "Internet of Things: A definition & taxonomy," in *Proc. 9th Int. Conf. Next Gener. Mobile Appl., Services Technol.*, Sep. 2015, pp. 72–77.

[2] A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges," *IEEE Access*, vol. 4, pp. 1375–1384, 2016.

[3] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, M. I. Jordan, and S. S. Sastry, "Kalman filtering with intermittent observations," *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1453–1464, Sep. 2004.

[4] W. Zeng and M. Y. Chow, "A trade-off model for performance and security in secured Networked Control Systems," in *Proc. IEEE Int. Symp. Ind. Electron.*, Jun. 2011, pp. 1997–2002.

[5] M. Stolpe, "The Internet of Things: Opportunities and challenges for distributed data analysis," *ACM SIGKDD Explor. Newslett.*, vol. 18, no. 1, pp. 15–34, 2016.

[6] Y. Jiang, S. Yin, and O. Kaynak, "Data-driven monitoring and safety control of industrial cyber-physical systems: Basics and beyond," *IEEE Access*, vol. 6, pp. 47374–47384, 2018, doi: 10.1109/ACCESS.2018.2866403.

[7] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd Annu. Design Autom. Conf.*, Jun. 2015, pp. 1–6.

[8] L. Cao, X. Jiang, Y. Zhao, S. Wang, D. You, and X. Xu, "A survey of network attacks on cyber-physical systems," *IEEE Access*, vol. 8, pp. 44219–44227, 2020, doi: 10.1109/ACCESS.2020.2977423.

[9] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in *Proc. 1st Workshop Secure Control Syst.*, 2010, pp. 1–6.

[10] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding schemes for securing cyber-physical systems against stealthy data injection attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 106–117, Mar. 2017.

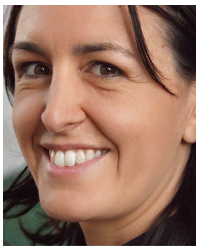
[11] F. Battisti, M. Carli, and F. Pascucci, "Securing cyber physical systems from injection attacks by exploiting random sequences," in *Proc. IEEE 13th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2017, pp. 1–6.

[12] F. Battisti, G. Bernieri, M. Carli, M. Lopardo, and F. Pascucci, "Detecting integrity attacks in IoT-based cyber physical systems: A case study on hydra testbed," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2018, pp. 1–6.
[13] S. S. Agaian, R. C. Cherukuri, and R. R. Sifuentes, "Key dependent covert communication system using fibonacci P-codes," in *Proc. IEEE Int. Conf. Syst. Syst. Eng.*, Apr. 2007, pp. 1–5.
[14] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes," in *Proc. 2nd ACM Int. Conf. Wireless sensor Netw. Appl. (WSNA)*, New York, NY, USA, 2003, pp. 151–159.
[15] O. Goldreich, *Foundations of Cryptography: Volume 2, Basic Applications*. New York, NY, USA: Cambridge Univ. Press, 2004.
[16] C. M. Medaglia and A. Serbanati, *An Overview of Privacy and Security Issues in the Internet of Things*. New York, NY, USA: Springer, 2010, pp. 389–395.
[17] NIST. (Jun. 2017). *Framework for Cyber-Physical Systems*. [Online]. Available: https://doi.org/10.6028/NIST.SP.1500-201
[18] M. Rostami, F. Koushanfar, and R. Karri, "A primer on hardware security: Models, methods, and metrics," *Proc. IEEE*, vol. 102, no. 8, pp. 1283–1295, Aug. 2014.
[19] L. Cazorla, C. Alcaraz, and J. Lopez, "Cyber stealth attacks in critical information infrastructures," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1778–1792, Jun. 2018.
[20] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, Jan. 2015.
[21] M. Krotofil, A. A. Cárdenas, B. Manning, and J. Larsen, "CPS: Driving cyber-physical systems to unsafe operating conditions by timing DoS attacks on sensor signals," in *Proc. 30th Annu. Comput. Secur. Appl. Conf. (ACSAC)*, New York, NY, USA, vol. 14, 2014, pp. 146–155.
[22] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 3023–3028, Nov. 2015.
[23] P. Srikantha and D. Kundur, "Denial of service attacks and mitigation for stability in cyber-enabled power grid," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2015, pp. 1–5.
[24] Z. Wang, L. Li, H. Sun, C. Zhu, and X. Xu, "Dynamic output feedback control of cyber-physical systems under DoS attacks," *IEEE Access*, vol. 7, pp. 181032–181040, 2019, doi: 10.1109/ACCESS.2019.2959083.
[25] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2009, pp. 21–32.
[26] C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," in *Proc. Amer. Control Conf.*, Jun. 2013, pp. 3344–3349.
[27] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011.
[28] G. Wu, J. Sun, and J. Chen, "A survey on the security of cyber-physical systems," *Control Theory Technol.*, vol. 14, no. 1, pp. 2–10, 2016.
[29] D. D. Wall, "Fibonacci series modulo m," *Amer. Math. Monthly*, vol. 67, no. 6, pp. 525–532, Jun. 1960.
[30] US Department of Defense, *The 'Orange Book' Series*. London, U.K.: Palgrave Macmillan, 1985.
[31] J. M. Taylor and H. R. Sharif, "Enhancing integrity of modbus TCP through covert channels," in *Proc. 11th Int. Conf. Signal Process. Commun. Syst. (ICSPCS)*, Dec. 2017, pp. 1–6.
[32] X. Ying, G. Bernieri, M. Conti, and R. Poovendran, "TACAN: Transmitter authentication through covert channels in controller area networks," in *Proc. 10th ACM/IEEE Int. Conf. Cyber-Phys. Syst.*, New York, NY, USA, Apr. 2019, pp. 23–34.
[33] J. Wu, Y. Tseng, and S. Huang, "An identity-based authenticated key exchange protocol resilient to continuous key leakage," *IEEE Syst. J.*, vol. 13, no. 4, pp. 3968–3979, Dec. 2019.
[34] H. Lin, H. Su, P. Shi, R. Lu, and Z. G. Wu, "Estimation and LQG control over unreliable network with acknowledgment randomly lost," *IEEE Trans. Cybern.*, vol. 47, no. 12, pp. 4074–4085, Dec. 2017.
[35] L. Wei and W. Yao, "Design and implement of LQR controller for a self-balancing unicycle robot," in *Proc. IEEE Int. Conf. Inf. Autom.*, Aug. 2015, pp. 169–173.

SARA BALDONI (Graduate Student Member, IEEE) received the bachelor's degree in electronics engineering and the master's degree in information and communication technology engineering from the University of Roma Tre, in 2016 and 2018, respectively. She is currently pursuing the Ph.D. degree in applied electronics with the Department of Engineering, University of Roma Tre. Her main research interests include communication security and navigation and localization systems.

FEDERICA BATTISTI (Senior Member, IEEE) received the Laurea (Master of Science) degree in electronic engineering and the Ph.D. degree from the University of Roma Tre, Rome, Italy, in 2006 and 2010, respectively. She is currently an Assistant Professor with the Department of Information Engineering, University of Padua. Her research interests include multimedia quality assessment and security. She serves as an Associate Editor for the IEEE TRANSACTIONS ON MULTIMEDIA, *EURASIP Journal on Image and Video Processing*, and *Signal Processing: Image Communication* (Elsevier).

MARCO CARLI (Senior Member, IEEE) received the Laurea degree in telecommunication engineering from the Università degli Studi di Roma "La Sapienza," Rome, Italy, and the Ph.D. degree from the Tampere University of Technology, Tampere, Finland. He was a Visiting Researcher with the Image Processing Laboratory, University of California, Santa Barbara, USA, from 2000 to 2004. He is currently an Associate Professor with the Department of Engineering, Università degli Studi Roma Tre. His research interests include digital signal and image processing with applications to multimedia communications, digital watermarking, multimedia quality evaluation, and information security.



FEDERICA PASCUCCI (Member, IEEE) received the M.S. degree in computer science and automation engineering from the University of Roma Tre, Rome, Italy, in 2000, and the Ph.D. degree in system engineering from the University of Rome La Sapienza, Rome, in 2004. She was a Visiting Scholar with Örebro University, Örebro, Sweden, in 2003, and the University of Cyprus, Nicosia, in 2013. Since 2005, she has been an Assistant Professor with the Department of Engineering, University of Roma Tre. She is currently the Principal Investigator in several EU funded projects. She has published over 80 journal and conference papers. Her current research interests include wireless sensor networks, indoor localization, cyber-physical systems, industrial control systems, and critical infrastructure protection. She was a recipient of the three best conference paper awards.