

Application of Correlation Indices on Intrusion Detection Systems: Protecting the Power Grid Against Coordinated Attacks

Christian Moya, *Student Member, IEEE*, Junho Hong, *Member, IEEE*, and Jiankang Wang, *Member, IEEE*

Abstract—The future power grid will be characterized by the pervasive use of heterogeneous and non-proprietary information and communication technology, which exposes the power grid to a broad scope of cyber-attacks. In particular, Monitoring-Control Attacks (MCA) –i.e., attacks in which adversaries manipulate control decisions by fabricating measurement signals in the feedback loop– are highly threatening. This is because, MCAs are (i) more likely to happen with greater attack surface and lower cost, (ii) difficult to detect by hiding in measurement signals, and (iii) capable of inflicting severe consequences by coordinating attack resources. To defend against MCAs, we have developed a semantic analysis framework for Intrusion Detection Systems (IDS) in power grids. The framework consists of two parts running in parallel: a Correlation Index Generator (CIG), which indexes correlated MCAs, and a Correlation Knowledge-Base (CKB), which is updated aperiodically with attacks’ Correlation Indices (CI). The framework has the advantage of detecting MCAs and estimating attack consequences with promising runtime and detection accuracy. To evaluate the performance of the framework, we computed its false alarm rates under different attack scenarios.

Index Terms—Power Grid, Cyber-Physical Systems, Cyber-Security, Monitoring-Control Attacks, Intrusion Detection Systems.

I. INTRODUCTION

THE power grid is evolving with increasing dependency on Information and Communication Technologies (ICT). Today, ICT is realized in energy control centers through Supervisory Control and Data Acquisition (SCADA) systems and Energy Management Systems (EMS). While EMSs make commands for power grid operation, SCADA systems serve as the gateway between EMS and field networks by passing measurements and control commands. The present SCADA is in the fourth generation of architectures, which bring innovative and cost-efficient solutions, such as cloud computing and Internet of Things, while opening up a much wider scope of cyber-security concerns among utilities [1]. Since the notorious Stuxnet attack to Siemens SIMATIC WinCC SCADA system in July 2010, approximately 45,000 cases of SCADA infection around the world have been reported, including the Iranian nuclear facilities and the Ukrainian power grid, according to Symantec’s statistics [2]. These attacks, if

successful, would lead to massive power outages, resulting in severe physical, economic, and social impacts.

Intrusion Detection Systems (IDS) are redeemed critical to protecting SCADA from cyber-attacks. In contrast to those methods aiming at strengthening the perimeter surrounding SCADA, IDSs generate ‘burglar alarms’ whenever the security of the system is compromised [3]. To increase the chances of mounting a successful defense, the Department of Homeland Security recommends a combination of firewalls, De-militarized Zones, and IDSs grounded on the principle of defense-in-depth [4].

While IDSs for traditional ICT systems are mature, implementing IDS in industrial control systems, such as power grids’ SCADA, is facing unprecedented challenges in twofold. First, the power grid is a cyber-physical system, wherein continuity of operation is critical. Unlike traditional ICT systems, in which the effects of false alarms are limited to computer operations, false alarms in power grids would disrupt dependent vital physical processes and inflict severe consequences. Therefore, false positive (which falsely generates alarms for normal actions) is unacceptable whereas low false negative rate is desired. Second, the power grid is a real-time dynamical system. Any delay of control actions could lead to instabilities from local plant angle instability to inter-area oscillation [5]. In the extremity, delayed response of protective devices will cause cascading blackouts over a large scale. For this reason, propagation latency of control and measurement signals induced from IDS audit and process must be minimized.

To address the first challenge, recent works develop IDS by integrating contextual information of power grids [6]–[12]. The most common approach is to identify attacks based on their impact on power grids. For example, in [12], Bayesian network models for the whole cyber-infrastructure and underlying power grids are constructed based on SCADA logs along with power network topological information. Power contingencies are then simulated on the Bayesian model to rank the severity of a detected cyber-intrusion. In [6], [10], [13], IDSs audit and select packets that contain control commands, which (dis)connect grid components, e.g., generators, transmission lines and substations. Cyber-attacks are identified if the power flow diverges in simulation under those control commands.

Another approach is to calibrate the detection results in cyber-space with historical data of power grid operation, wherein data mining techniques are often applied. For example, deviations between current and historical Area Control

C. Moya and J.K. Wang are with the Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH, 43210 USA e-mail: {moyacalderon.1,wang.6536}@osu.edu.

J. Hong is with the Energy and Automation Department, ABB US Corporate Research Center, Raleigh, NC, 27519 USA e-mail: junho.hong@us.abb.com.

Errors are used as indicators of cyber-attacks to Automatic Generation Control in EMS [9]. A hybrid IDS is developed in [7] that learns temporal state-based specifications for power grid scenarios of physical disturbances, cyber-attacks, and normal operations.

However, both of these approaches share the common deficiency of requiring a long runtime, exacerbating the second challenge. While the former approach simulates power grids' response, which is a non-trivial task given the enormous size of power networks and the number of grid devices, the latter approach relies on frequent auditing and processing historical data over a sufficiently long period in order to ensure the desired accuracy. These put a high requirement on IDS accounting resources and could significantly reduce IDSs' performance in timely processing and propagating the information to grid functions and responsible defense authorities.

Despite initial attempts on reducing IDS runtime in [6], [14], they are restricted to certain attack groups, wherein attacks are aimed at individual grid components and assume a single step in the cyber-physical causal chain (*i.e.*, adversaries directly disconnect grid devices through remote control); they are not able to handle more sophisticated attacks that are coordinated and through EMS. These attacks are defined as *Monitoring-Control Attacks (MCA)* and considered highly threatening [15], because they are (i) more likely to happen with greater attack surface and lower attack cost, (ii) difficult to detect by hiding in measurement signals and masquerading through EMS, and (iii) capable of inflicting much more severe consequences at a greater scale by coordinating attack resources targeting at multiple grid components. Although MCAs' attack mechanisms and physical impacts have been studied in a few works [16]–[19], there is no effective IDS solution available to defend against MCAs.

To bridge this gap, this paper presents a semantic analysis framework for IDSs in power grids, which detects MCAs with promising runtime and detection accuracy. The framework is implemented as two parts running in parallel in IDS: a Correlation Index Generator (CIG), which indexes correlated attacks, and a Correlation Knowledge-Base (CKB), which is updated aperiodically with attacks' Correlation Indices (CI). In addition, this paper makes the following contribution:

- A theoretical basis for CIG. We formulate MCAs as a bi-level mix-integer optimization program and solve it to provide CI solutions.
- A suite of detection rules for CKB. Derived from set theory, these rules characterize the relation between adversaries' goals and coordinated attacks, thus enabling CKB to detect MCAs at runtime.
- Defense strategies against MCAs. While most IDSs are passive, that is, they only generate “burglar alarms”, our proposed method actively derives defense strategies against MCAs using a set-theoretic approach.

The rest of the paper is organized as follows. Section II introduces the threat model, MCAs mechanisms and IDS implementation of the proposed semantics framework. Section III presents the mathematical model of power grids and MCAs. The theoretic basis for CIG and detection rules for CKB are derived in Section IV and V. In Section VI, the performance of

proposed semantic framework is demonstrated with numerical experiments. Finally, all results of this paper are concluded in Section VII. While the proposed framework is capable of defending against less sophisticated attacks, such as control attacks, we elaborate the framework's working principle mainly based on MCAs in this paper.

II. BACKGROUND

In order to develop the semantic analysis framework for IDSs in power grids, we need to consider three factors: the environment in which intrusions occur (the threat model), the intrusions we wish to detect (MCAs), and the intrusion detector (IDS implementation).

A. Threat Model

In the previous generations, SCADA activities were basically confined to proprietary networks. In contrast, the current fourth generation of SCADA is mostly internet-based, as illustrated in Fig. 1. In particular, a large amount of measurement signals from transducers of grid equipment (*e.g.*, relays, generators and switch gears) are transmitted with raw data protocol in field networks [3]. This widens the cyber-attack surface in the following attack entry points as numbered in Fig. 1 [1]:

- (1) Directly hack into field devices, including transducers, actuators and meters.
- (2) Attack field network links between devices and from devices to Energy Control Centers (ECC).
- (3) Attack from inside of the ECC. This could happen within or external of the security enclaves, which boundaries are defined by the trust nodes (*e.g.*, firewall and IDS) [20].
- (4) Attack from inside enterprises functions or attack at its perimeter networks.

Through these channels, adversaries can install malware, sniff, inject and modify host files and network traffic [1], [21], [22]. Based on the above fact, we make the following assumptions about the threat model:

- 1) Adversaries can remotely penetrate the Local Area Network (LAN) and Wide Area Network (WAN). Though insider attacks outside security enclaves are allowed under the proposed framework, it is not our focus. We do not consider insider attacks within the security enclaves.
- 2) In ECC, we trust EMS. In other words, attacks are only executed on packets containing control and measurement signals that are transmitted over the network; they do not damage the EMS functions nor alter its encoded working principles.
- 3) IDSs are secure (*i.e.*, not compromised). In addition, we assume there are separate computing machines dedicated to IDSs that implement the proposed semantic analysis framework. Therefore, IDSs do not introduce extra vulnerabilities into power grids.
- 4) IDS communication is secure. In other words, IDSs can safely exchange data.
- 5) We do not consider attacks through enterprises functions. Launching MCAs through this path, though theoretically possible, is much more likely to fail due to extra layers of trust nodes.

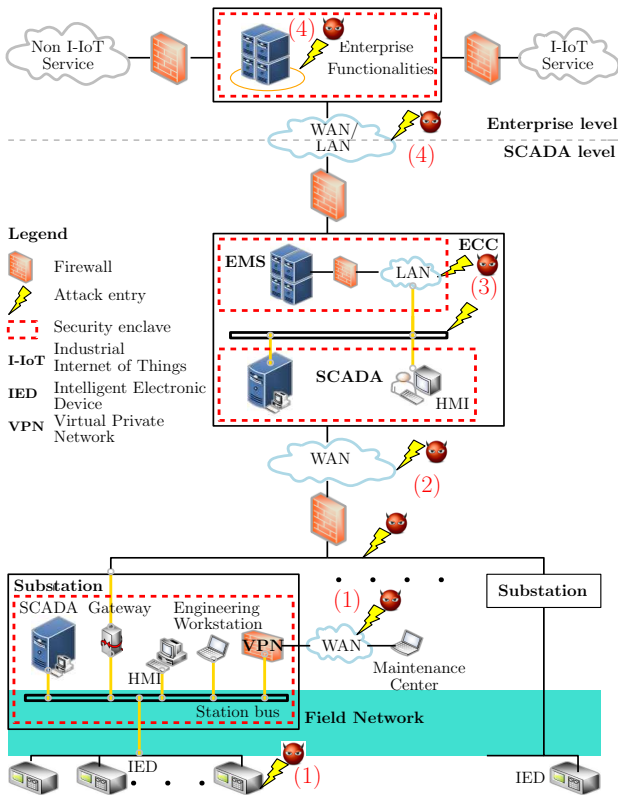


Fig. 1. EMS/SCADA Power Grid and Attack Entry Points.

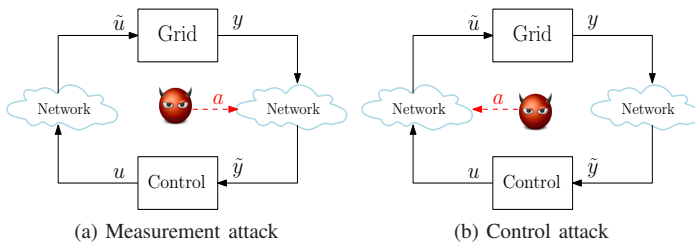


Fig. 2. Control and measurement attacks. u : control command, y : measurements. $u \neq \hat{u}$ ($y \neq \hat{y}$) during the cyber-attack, where \hat{u} and \hat{y} are the corrupted control and measurement signals.

B. Monitoring-Control Attacks

There are two classes of attack mechanisms in power grids, control attacks and monitoring attacks [15]. They are illustrated in with a generic control diagram in Fig. 2. Control attacks refer to attacks that directly hijack and falsify control commands in power grids, such as disconnecting transmission lines and changing the power output of generators [6], [14], [21]. While able to inflict immediate physical consequences, they are less likely to occur in practice due to the restricted communication channels and easiness of detection. For example in conventional substations, relay commands, which trigger circuit breakers, are usually transmitted over proprietary communication channels or hard wire connection; generator power adjustments are requested through Human Machine Interface (HMI), where operators would block and report suspicious actions.

Monitoring attacks contaminate or eavesdrop measurements collected from transducers. In contrast to control commands, measurement signals have been more often transmitted over

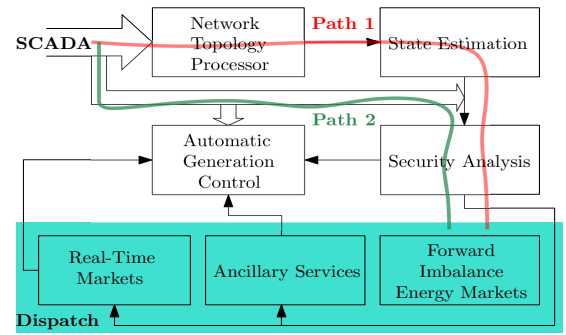


Fig. 3. Attack Paths on EMS. In path 1, the adversary go through State Estimation and its screening methods. In path 2, the adversary can inject any attack signal that deceives the operator.

open-communication channels (*i.e.*, without any available authentication method) due to their large transmission volume and high transmission rate. This opens a wider cyber-surface to attacks. An important subset of monitoring attacks is *Monitoring-Control Attacks*, in which adversaries manipulate control decisions by fabricating measurement signals in the feedback loop. On one hand, MCAs are difficult to detect, since the attack goals are hidden behind measurements and the control mechanisms. Thus, they cannot be inspected and intervened by human operators. On the other hand, they can inflict severe consequence by coordinating attack resources targeting at many measurements simultaneously; they are different from non-disruptive monitoring attacks that only exploit private information. Therefore, MCAs are considered highly threatening.

MCAs' mechanism in power grids is briefed next. Main control functions of the power grid are realized through EMS, which consists of four blocks: network model-building (including topology processor and state estimation), security assessment, automatic generation control, and dispatch. Information flows within EMS are shown in Fig. 3. In path 1, contaminated measurements drive control decisions in automatic generation control and dispatch after going through network-building models. While state estimation could effectively correct and identify bad data, a rich body of literature has demonstrated that contaminated measurements can still be injected through when the measurement errors are within the tolerance and/or the measurements are structure-wise conforming [23]–[25]. In path 2, contaminated measurements directly drive control decisions, as it is common for system operators to make a decision based on raw measurements in security constrained dispatch. Through both paths, adversaries may realize goals, such as depriving profit in electricity markets, disturbing power grid frequency and overloading grid equipment, causing tremendous financial losses, sabotaging, or even interrupting continuous grid operation.

C. IDS Implementation

1) *Proposed Framework in IDS Architecture*: A general IDS architecture is defined with four modules, Event (E-blocks), Analysis (A-blocks), Database (D-blocks), and Response (R-blocks), as shown in Fig. 4 [26]. The proposed semantic analysis framework has two parts: Correlation Index

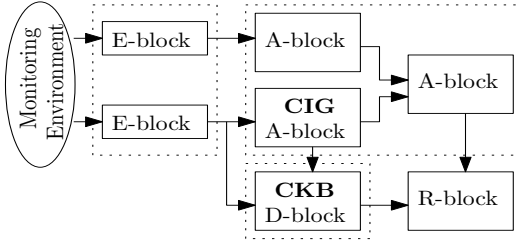


Fig. 4. Proposed IDS working principles [26]. E-blocks are Event blocks/IDSs' sensors, A-blocks are analysis blocks, D-blocks are database blocks, and R-blocks are response or mitigation blocks. In particular, CIG is an A-block and CKB is a D-block.

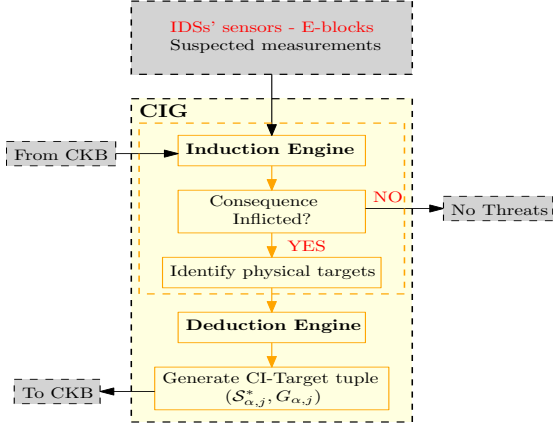


Fig. 5. Correlation Index Generator (CIG).

Generator (CIG) and Correlation Knowledge Base (CKB). They are aimed to provide contextual information of power grids additional to the traits that IDS sensed in the cyber-space (e.g., host syslog and network traffic).

CIG, depicted in Fig. 5, belongs to A-blocks. It analyzes the correlation of the potential hostile behaviors sensed by E-blocks, and indexes these behaviors with inductive-deductive patterns. For example, if a set of measurements are suspected to be contaminated, CIG first induces their consequence on the power grid with optimal power flow. If a transmission line is overloaded, then these measurements are *weakly correlated*. Next, CIG deduces the critical measurements required to overload the transmission line. These critical measurements are *strongly correlated* and will be represented by a set of Correlation Indices (CI). The inductive-deductive patterns ensure minimal false negative rates that might be caused by normal deviations, such as noises and faults. In addition, CIG can be used to protect critical grid assets from MCAs, in which case CIs can be directly deduced from the predicted failures of these assets. Details about CIG are provided in Section IV.

CKB, depicted in Fig. 6, belongs to D-blocks. It is updated with the CIs generated from CIG at an adaptive rate, which is determined by (i) configuration change of power networks, (ii) power grid stress level, (iii) detection rate of potential hostile events of E-blocks, and (iv) human operator's settings. At runtime, measurements detected by E-blocks are compared with the CIs in CKB. If the comparison is positive, then these measurements are considered forming an MCA. This

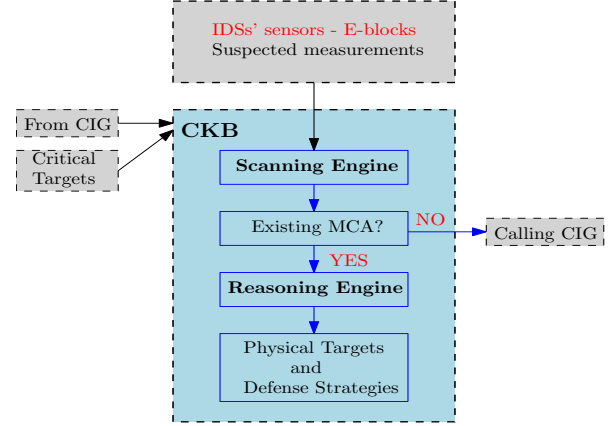


Fig. 6. Correlation Knowledge Base (CKB).

information is passed to other A-blocks and R-blocks for further response. Since CKB does not contain any computation function, apart from arithmetic operation for CI comparison, it allows fast contextual information integration in IDSs. Details about CKB are provided in Section V.

Derived from set theory, defense strategies are proposed for R-blocks. The design of E-blocks is out of the scope of this paper.

2) *IDS Dimensions*: We consider two dimensions of IDS implementation related to the proposed semantic analysis framework. The proposed framework is flexible in implementation in the other dimensions, such as audit source (i.e., host- or network-based detection), audit frequency and continuity, which definitions are given in the survey [27].

Detection Approach. There are two main detection approaches in IDS development: signature- and anomaly-based. In between these approaches lie the probabilistic- and specification-based methods [1], [27], [28]. All of these approaches are based on *direct* knowledge of cyber-activities (i.e., host syslog and network traffic). In complementary, behavioral detection approaches capture the patterns, which are not necessarily illegitimate in a direct setting but wrong in a *contextual* setting as a secondary evidence. The proposed analysis framework belongs to the last class and will be implemented with other direct knowledge-based approaches in IDS.

Distributed v.s. Centralized. The proposed analysis framework can be implemented under centralized, distributed or hierarchical structure of IDS. Provided the cost and communication constraints in power grids, we consider IDSs are only installed at the substation level and above, but not at individual Intelligent Electronic Devices or Remote Terminal Units. Thus, under a centralized structure, the proposed framework will allow IDS at a substation to detect and identify MCAs within its service area. For MCAs across service areas under multiple substations, a distributed structure is needed, wherein IDS at substations have peer-to-peer communication so that detected events can be exchanged. Alternatively, a hierarchical structure can be formed. The proposed analysis framework is integrated at a master IDS, which supervises all the substation IDSs by collecting, analyzing their detected events and sending instructions for detected MCAs.

III. MATHEMATICAL MODELS

In this section, we model the power grid, dispatch applications, and Monitoring Control Attacks.

A. Mathematical Notation

Throughout this paper, we use the following mathematical notation. Let \mathbb{R} and $\mathbb{R}_{\geq 0}$ (resp. $\mathbb{R}_{> 0}$) denote the set of real numbers and the set of non-negative (resp. positive) real numbers. We let $\mathbf{1}$ and $\mathbf{0}$ denote, respectively, the vectors or matrices with all components equal to one and zero. Given a finite set V , we let $|V|$ denote its cardinality, *i.e.*, the number of elements of V , and 2^V the power set of V , *i.e.*, the set of all subsets of V .

For a matrix $A \in \mathbb{R}^{n \times m}$, we let $[A]_i$ denote its i th row. For a vector $x \in \mathbb{R}^n$, x_i denotes its i th element, $\text{diag}(x)$ the diagonal matrix of x , and $\|x\|_0$ the zero-norm of x , *i.e.*, the number of non-zero elements of x .

B. Power Grid Model

We model the power grid as the graph $G = (V, E)$, where V is the set of n buses and $E \subset V \times V$ is the set of m transmission lines. To each bus $i \in V$, we associate the demand (or consumption) $P_{d,i} \in \mathbb{R}_{\geq 0}$. In addition, let $V_g \subset V$ denote the set of n_g buses with dispatchable generation. To each generator bus $i \in V_g$, we associate the power generated $P_{g,i} \in \mathbb{R}_{> 0}$. Similarly, to each transmission line $l := (i, j) \in E$ connecting buses i and j , we associate the power flow $P_{f,l} \in \mathbb{R}$. In vector form, the demand, generation, and power flows are, respectively, $P_d = [P_{d,1}, P_{d,2}, \dots, P_{d,n}]^\top$, $P_g = [P_{g,1}, P_{g,2}, \dots, P_{g,n_g}]^\top$, and $P_f = [P_{f,1}, P_{f,2}, \dots, P_{f,m}]^\top$.

The power grid is assumed to have a set of n_s substations, *i.e.*, $S := \{s_1, s_2, \dots, s_{n_s}\}$. We model the power grid within substation s_k 's service area as the sub-graph $G_{s_k} = (V_{s_k}, E_{s_k})$ with the following properties:

- 1) All substations' service areas compose the power grid, *i.e.*, $G = \cup_{s_k \in S} G_{s_k}$.
- 2) Substations' service areas might overlap, *i.e.*, for some $s_j, s_k \in S$, we may have $G_{s_j} \cap G_{s_k} \neq \emptyset$.
- 3) The overlapped areas do not contain generator buses.
- 4) Each substation s_k collects demand measurements, denoted as $\tilde{P}_d \in \mathbb{R}_{\geq 0}^n$, within its service area, *i.e.*, all \tilde{P}_d, i such that $i \in V_{s_k}$.

C. Dispatch Application Model

Dispatch applications in EMS compute the generation output for the grid, denoted as $P_g^+ \in \mathbb{R}_{> 0}^{n_g}$, by observing demand measurements \tilde{P}_d and using security constrained optimal power flows. These applications are triggered based on a guard condition (*i.e.*, a boolean condition). This guard condition is enabled by a security assessment algorithm (which usually involves network model-building), or by a system operator during real-time and contingency dispatch. Examples include generation dispatch in Real-Time Markets and Ancillary Services (see Fig. 3).

Dispatch applications are based on the active and reactive power flow model, which describes how power balances on

buses and flows on transmission lines. However, computing this coupled power flow may become computationally intractable for large-scale power grids. For this reason, the decoupled DC power flow is commonly adopted by operators when the power grid is in the normal status [29]. The linearity and sparsity in the DC power flow allows much faster computation.

We formulate the security constrained DC optimal power flow as a convex optimization problem that minimizes the generation cost (1a), balances generation and demand (1b), and keeps the generation (1c) and power flows (1d) within operational limits, *i.e.*,

$$\Omega(\tilde{P}_d) : \min_{P_g} \frac{1}{2} P_g^\top C_2 P_g + c_1^\top P_g + c_0, \quad (1a)$$

$$\text{s.t. } \mathbf{1}^\top P_g - \mathbf{1}^\top \tilde{P}_d = 0, \quad (1b)$$

$$P_g \in [\mathbf{0}, \bar{P}_g], \quad (1c)$$

$$\underbrace{F(\Pi_g P_g - \tilde{P}_d)}_{=: P_f} \in [-\bar{P}_f, \bar{P}_f], \quad (1d)$$

where $c_0, c_1, c_2 \in \mathbb{R}_{\geq 0}^n$ are the cost coefficients for generators, $C_2 = \text{diag}(c_2)$, $\bar{P}_g \in \mathbb{R}_{\geq 0}^n$ is the rated power from generators, $\bar{P}_f \in \mathbb{R}_{\geq 0}^m$ is the thermal capacity of transmission lines, $F \in \mathbb{R}^{m \times n}$ is the generator shift matrix, and $\Pi_g \in \{0, 1\}^{n \times n_g}$ is a matrix that maps generator buses to buses.

Thus, given the demand measurements \tilde{P}_d , an optimal solution $P_g^+ \in \Omega(\tilde{P}_d)$ corresponds to the new generation output for the grid.

D. Attack Model

In this subsection, we define MCAs, attack goals, and attack constraints. We also describe two types of MCAs: strongly and weakly correlated.

Monitoring Control Attacks: MCAs aim to manipulate dispatch applications in EMS. In an MCA, adversaries hack into substations' ICT. The corrupted measurements are modeled as follows:

$$\tilde{P}_d(a) = P_d + a, \quad (2)$$

where $a \in \mathbb{R}^n$ denotes the difference between the attack signal $\tilde{P}_d(a)$ and the actual signal P_d .

Attack Goal: The adversary uses these MCAs to manipulate (1), so the new (deceived) generation output $P_g^+(a) \in \Omega(\tilde{P}_d(a))$ increases the power flows on a set of target lines $L \subset E$. Therefore, the attack goal is denoted as,

$$G_{\alpha,j} := \{(l, \tau_l) : [F]_l(\Pi_g P_g^+(a) - P_d) \geq (1 + \tau_l) P_{f,l}(0)\}. \quad (3)$$

where $G_{\alpha,j} \subset E \times \mathbb{R}_{> 0}$ is the attack goal, $[F]_l$ is the l th row of the generation shifting matrix, $P_{f,l}(0)$ denotes the power flow on line $l \in L$ before the MCA, and $\tau_l \in \mathbb{R}_{> 0}$ quantifies the flow increase on $l \in L$. We choose this flow increase τ_l with semantics, including the flow increase that congests a transmission line or trips the line's protection.

Attack Constraints: MCAs are constrained based on the path they take on EMS. If the attack takes path 1 (see Fig. 3), the MCA gets through state estimation and its data screening method. If the attack takes path 2 (see Fig. 3), the MCA must take any value that deceives the operator. In any case, we can model this constraint as

$$a \in [-\bar{a}, \bar{a}]. \quad (4)$$

In the above, $\bar{a} \in \mathbb{R}_{\geq 0}^n$ is the vector of max values allowed for the attack signal. We can use this vector to design different attack scenarios.

Remark 1. *The constraint for path 1 can take a form that explicitly describes the condition under which measurement attacks get through state estimation and its data screening methods. These methods, however, are not used during real-time and contingency dispatch (Path 2).*

MCAs are also constrained by defense at substations. If the grid's operator deploys defense at substation s_k , the adversary cannot corrupt its measurements. We model this constraint as

$$a_i \in \delta_{s_k} [-\bar{a}_i, \bar{a}_i], \quad \forall i \in V_{s_k}, \quad \forall s_k \in S, \quad \delta_{s_k} \in \{0, 1\}. \quad (5)$$

where $\delta_{s_k} = 1$ if measurements at substation s_k are corruptible and $\delta_{s_k} = 0$ if not. The vector $\delta = [\delta_{s_1}, \delta_{s_2}, \dots, \delta_{s_{n_s}}]^\top$ describes target and safe substations during MCAs. Using δ , we can identify the set of target/attacked substations as follows

$$S_{\alpha,j} := \{s_k \in S : \delta_{s_k} = 1\} \in 2^S.$$

Note that we can also use (5) to model the desire (for the adversary) to attack substation s_k .

Finally, MCAs are constrained by the adversary's resources. If the adversary has limited resources, (s)he can only attack (hack) a limited number of substations. We model this constraint as

$$\|\delta\|_0 \leq \kappa, \quad \kappa \in \{1, 2, \dots, n_s\}. \quad (6)$$

In the worst case scenario for the operator, the adversary minimizes κ .

Types of Coordinated MCAs: Since the power grid is built with redundant measurements, attacking measurements in a single substation may not induce any consequence. In other words, effective MCAs are usually launched as a coordinated effort, which consists of temporally and spatially correlated events. Given the attack goal $G_{\alpha,j}$, we classify coordinated MCAs as strongly and weakly correlated. *Strongly Correlated MCAs*, denoted as $S_{\alpha,j}^* \in 2^S$, achieve $G_{\alpha,j}$ by attacking the least number of substations. Strongly correlated MCAs describe attacks with minimum resources and allow us to predict attack consequences and derive defense implications. In Section IV, we will introduce a formal method to model and study strongly correlated MCAs. On the other hand, *Weakly Correlated MCAs*, denoted as $S_{\alpha,j} \in 2^S$, achieve $G_{\alpha,j}$ by attacking more substations than needed. Adversaries execute weakly correlated MCAs to probe defense at substations.

IV. CORRELATION INDEX GENERATOR

In this section, we describe the working principles of the Correlation Index Generator (see Fig. 5) and its components, namely the Induction Engine and the Deduction Engine.

A. Induction Engine

Suppose the E-blocks detected an MCA $S_{\alpha,j} \in 2^S$ that is not in CKB and has corrupted measurements $\tilde{P}_d(a)$. The *induction engine* computes the new (deceived) generation output $P_g^+(a)$ by solving $\Omega(P_d + a) =: \Omega(\tilde{P}_d(a))$, i.e.,

$$\begin{aligned} \Omega(\tilde{P}_d(a)) : \min_{P_g} & \quad \frac{1}{2} P_g^\top C_2 P_g + c_1^\top P_g + c_0, \\ \text{s.t.} & \quad \mathbf{1}^\top P_g - \mathbf{1}^\top (P_d + a) = 0, \\ & \quad P_g \in [\mathbf{0}, \bar{P}_g], \\ & \quad F(\Pi_g P_g - (P_d + a)) \in [-\bar{P}_f, \bar{P}_f]. \end{aligned}$$

Then, using $P_g^+(a) \in \Omega(\tilde{P}_d(a))$, the *induction engine* determines the set of attack consequences, i.e., the set $G_{\alpha,j}$. As shown in (3), the set of consequences $G_{\alpha,j}$ depends on τ_l and P_d . The flow increase τ_l is chosen with semantics and the real consumption P_d is obtained as follows.

$$P_{d,i} := \begin{cases} \tilde{P}_{d,i}, & \text{if } i \notin V_{s_k}, \quad \forall s_k \in S_{\alpha,j}, \\ P_{d,i}^{\text{pre}}, & \text{otherwise,} \end{cases}$$

where $P_{d,i}^{\text{pre}}$ is a (conservative) estimated consumption or a redundant measurement.

B. Deduction Engine

Given the set of consequences inflicted $G_{\alpha,j}$, the *deduction engine* computes strongly correlated MCAs that reach $G_{\alpha,j}$ using the following bilevel mix-integer optimization program:

$$\min_{P_g^+, a, \kappa, \delta} \quad \kappa, \quad (7a)$$

$$\text{s.t.} \quad \text{equations (2) - (6)}, \quad (7b)$$

$$P_g^+ \in \Omega(\tilde{P}_d(a)). \quad (7c)$$

In our previous work [30], we derived a method that addresses the mathematical challenges of (7) and computes strongly correlated MCAs. The method first computes the security index, which corresponds to the optimal solution κ^* . This security index describes the minimum number of substations the adversary must attack to reach $G_{\alpha,j}$. Then, the method determines the target and safe substations during the MCA from the optimal solution δ^* . Since δ^* is not necessarily unique, we proposed in [30] an algorithm to determine all feasible solutions δ^* such that $\|\delta^*\|_0 = \kappa^*$. All these δ^* correspond to strongly correlated MCAs associated with the attack goal $G_{\alpha,j}$.

We use a set-theoretic approach to describe all these strongly correlated MCAs, which we define as Correlation Indices.

Definition 1. *Let δ^* denote a feasible solution of (7) associated with $G_{\alpha,j}$ such that $\|\delta^*\|_0 = \kappa^*$. A Correlation Index (CI), denoted as $S_{\alpha,j}^*$, is a strongly correlated MCA that extracts target substations from δ^* as follows*

$$S_{\alpha,j}^* := \{s_k \in S : \delta_{s_k}^* \neq 0\} \in 2^S,$$

and inflicts the consequences described by $G_{\alpha,j}$.

The set of all CIs associated with the inflicted consequences $G_{\alpha,j}$ is given by $S_{\alpha,j}^* := \{S_{\alpha,j}^* : S_{\alpha,j}^* \text{ is a CI}\}$.

As a result, the CIG generates a *CI-target tuple* $(S_{\alpha,j}^*, G_{\alpha,j})$ –i.e., the set of strongly correlated MCAs and the associated inflicted consequences– and sends this CI-target tuple to the Correlation Knowledge-Base (CKB).

V. CORRELATION KNOWLEDGE-BASE

In this section, we describe the working principles of the Correlation Knowledge-Base (CKB) (see Fig. 6) using a set-theoretic approach. The CKB has a Scanning Engine and a Reasoning Engine.

A. Scanning Engine

Suppose the E-blocks detected a (possibly weakly correlated) MCA $S_{\alpha,j}$. The *Scanning Engine* verifies if $S_{\alpha,j}$ is an existing MCA, i.e., if $S_{\alpha,j} \in \text{CKB}$. The MCA $S_{\alpha,j}$ is an existing MCA if

- 1) The MCA is a CI (or strongly correlated MCA), i.e., $S_{\alpha,j} \in S_{\alpha,j}^*$ for some $S_{\alpha,j}^* \in \text{CKB}$.
- 2) The MCA is a weakly correlated MCA but a superset of at least one CI, i.e., $\exists S_{\alpha,j}^* \subset S_{\alpha,j}$ such that $S_{\alpha,j}^* \in \text{CKB}$.
- 3) The MCA is uncorrelated, is a subset of at least one CI, i.e., $\exists S_{\alpha,j}^* \supset S_{\alpha,j}$ such that $S_{\alpha,j}^* \in \text{CKB}$, and has less cardinality than all CIs in CKB, i.e., $|S_{\alpha,j}| < |S_{\alpha,j}^*|$ for all $S_{\alpha,j}^* \in \text{CKB}$.

If $S_{\alpha,j}$ is an existing MCA, then CKB uses the reasoning engine to identify physical targets and derive defense strategies. Otherwise, CKB calls the CIG to analyze $S_{\alpha,j}$.

B. Reasoning Engine

The *reasoning engine* identifies physical targets and derives defense strategies for the detected MCA $S_{\alpha,j}$. Technically, the reasoning engine is an R-block (see Fig. 4) and can work also with CIG to derive defense strategies.

To identify physical targets associated with $S_{\alpha,j}$, we proceed as follows.

- 1) If the MCA $S_{\alpha,j}$ is a CI, then the physical targets are described by the set of inflicted consequences $G_{\alpha,j}$.
- 2) If the MCA $S_{\alpha,j}$ is a weakly correlated MCA that contains a set of $q \geq 2$ CIs, i.e., the set

$$S_{\text{CI}} := \{S_{\alpha,j}^* : j = 1, \dots, q \text{ and } S_{\alpha,j}^* \subset S_{\alpha,j}\},$$

then the physical targets are given by the union of the inflicted consequences associated with each CI, i.e., $\cup_{j=1}^q G_{\alpha,j}$ where $(S_{\alpha,j}^*, G_{\alpha,j})$ is a CI-tuple of an existing MCA.

To derive defense strategies against $S_{\alpha,j}$, we proceed as follows.

- 1) If the MCA $S_{\alpha,j}$ is a CI, then the best defense strategy is to defend any substation.

This defense will render the attack ineffective, which we justify next.

Proposition 1. (*Defense against strongly correlated MCAs*) Let $S_{\alpha,j}$ denote a strongly correlated MCA. If the operator protects measurements at any substation s_k^* such that $s_k^* \in S_{\alpha,j}$, the attack $S_{\alpha,j} \setminus \{s_k^*\}$ becomes ineffective.

Proof. See Appendix. \square

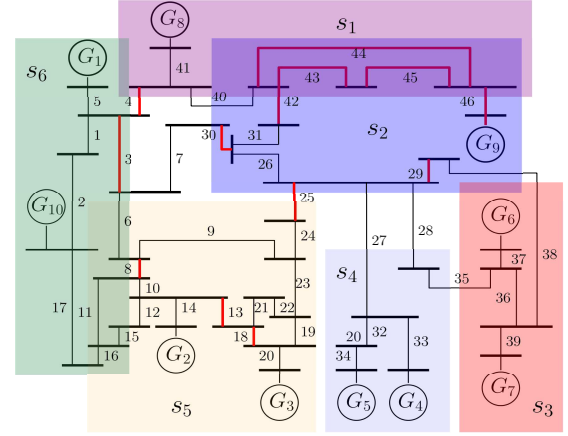


Fig. 7. New England 39-bus system.

- 2) If the MCA $S_{\alpha,j}$ is a weakly correlated MCA that contains the set of CIs S_{CI} , then we may have one of the following cases.

Case I: If $\cap_{j=1}^q S_{\alpha,j}^* \neq \emptyset$, then the best defense strategy is to protect measurements at substation s_k^* that satisfies $s_k^* \in \cap_{j=1}^q S_{\alpha,j}^*$, which we justify next.

Proposition 2. (*Defense against a set of strongly correlated MCAs with non-empty intersection*) Let $S_{\alpha,j}$ denote a weakly correlated MCA that contains the set of CIs S_{CI} . Suppose these CIs satisfy $\cap_{j=1}^q S_{\alpha,j}^* \neq \emptyset$. If the operator protects measurements at a substation s_k^* such that $s_k^* \in \cap_{j=1}^q S_{\alpha,j}^*$, the attack $S_{\alpha,j} \setminus \{s_k^*\}$ becomes ineffective.

Proof. Follows from Proposition 1. \square

Case II: If $\cap_{j=1}^q S_{\alpha,j}^* = \emptyset$, then the best strategy is to defend all CIs individually, which we justified using Proposition 1.

Case III: Finally, there is an intermediate case in which only some CIs have a non-empty intersection. For this case, a combination of the defense strategies described for Case I and II should be implemented.

VI. NUMERICAL EXPERIMENTS

In this section, we use numerical experiments to validate our proposed framework. In particular, we compute the false alarm rates for CIG and CKB under different attack scenarios.

A. Experimental Setup

We describe the experimental environment, the IDS benchmark systems, and the evaluation metric next.

1) *Environment:* We model a power grid with $n_s = 6$ substations using the New England 39-bus system illustrated in Fig. 7. We model the dispatch application using the DC Optimal Power Flow tool from MatPower [31]. The data used for the power grid and dispatch application corresponds to Matpower base-case data.

In our experiments, we used the adversarial environment introduced in [32]. This adversarial environment is characterized by a nominal attack rate (or attack intensity) $p_0 \in (0, 1)$, which E-blocks estimate as \hat{p}_0 .

We model MCAs using a random approach, that is, we selected the corrupted measurements $\tilde{P}_d(a)$ and target substations $S_{\alpha,j}$ uniformly at random. In particular, $\tilde{P}_d(a)$ was chosen uniformly from the interval $[P_d - \bar{a}, P_d + \bar{a}]$ where $\bar{a} = 0.1P_d$. This random approach allowed us to model attack events that are a threat and attack events that are not.

2) *Intrusion Detection Systems*: We model E-blocks (or IDS's detector) with the following characteristics. The E-blocks have a detection rate $p_D \in (0, 1)$ and a false alarm rate $p_{FA} \in (0, 1)$. In our experiments, we selected the values of $p_D = 0.9$, $p_{FA} = 0.1$. The adversary attempts to manipulate the E-blocks' p_D , p_{FA} , and \hat{p}_0 by using the following parameters:

- δ : the maximum deviation under \hat{p}_0 .
- β : the maximum probability to launch a zero-day (*i.e.*, undetectable) attack.
- α : the maximum probability to intentionally trigger a false alarm.

In the simulation, we selected the values $\delta = 0.1\hat{p}_0$, $\beta = 0.2$, $\alpha = 0.1$, and $\hat{p}_0 \in \{0.25, 0.1, 0.05\}$.

We model two benchmark IDSs, a simple IDS (IDS-1) and a Bayesian IDS (IDS-2). IDS-1 has the following working principle. If the E-blocks trigger an alarm, IDS-1 will label the event as an intrusion. IDS-2, on the other hand, has the following working principle. An event is labeled as an intrusion based on $\mathbb{P}(\text{Intrusion}|\text{Alarm})$, *i.e.*, the probability of intrusion given that an alarm has been triggered. This probability is computed as follows

$$\mathbb{P}(I|A) = \frac{\mathbb{P}(A|I)\mathbb{P}(I)}{\mathbb{P}(A|I)\mathbb{P}(I) + \mathbb{P}(A|\neg I)\mathbb{P}(\neg I)},$$

where A denotes the alarm and I intrusion. Since $\mathbb{P}(I) = \hat{p}_0$, $\mathbb{P}(A|I) = p_D$, $\mathbb{P}(\neg I) = 1 - \hat{p}_0$, and $\mathbb{P}(A|\neg I) = p_{FA}$; we write $\mathbb{P}(I|A)$ as

$$\mathbb{P}(I|A) = \frac{p_D \hat{p}_0}{(p_D - p_{FA})\hat{p}_0 + p_{FA}}, \quad (8)$$

which is also known as the *Bayesian detection rate* [32].

To model CKB and CIG, we proceed as follows. For CKB, we computed CI-tuples for each experiment using CVX and Gurobi, packages for specifying and solving convex and mix-integer programs [33]. CIG detects possible threats based on deviation from the pseudo-measurements P_d^{pre} , which are generated from a uniform distribution in $[0.9P_d, 1.1P_d]$. We assume no redundant measurements are available for CIG to replace the corrupted measurements. Nevertheless, if they are available, the false alarms (for CIG) will tend to 0.

CKB and CIG will label an incoming MCA as a threat, if the attack can increase the flow $\tau_l = 15\%$ in any of the following target lines $L = \{3, 4, 13, 18, 25, 29, 30, 42, 43, 44, 45, 46\}$ (see Fig. 7). This requires for CKB to have CI-tuples for each line $l \in L$.

3) *Metrics*: The performance of the benchmark IDSs and the proposed framework is measured by the false negative rate $\text{FNR} := \text{FN}/(\text{TP} + \text{FN})$, where FN denotes the false negatives (*i.e.*, failure of generating an alarm) and TP the true positives (*i.e.*, success of generating an alarm correctly), and the false positive rate $\text{FPR} := \text{FP}/(\text{TN} + \text{FP})$, where FP denotes the

false positives (*i.e.*, generating a false alarm) and TN the true negatives (*i.e.*, stay silent when there is no event).

We further define these metrics for intrusions that are not a threat (*i.e.*, *ineffective attacks*) and for intrusions that are a *threat* (denoted as FNR_t and FPR_t). Since IDS-1 and IDS-2 are not capable of estimating attack consequences and determining possible threats, we compute FNR_t and FPR_t only for the proposed framework. All metrics are evaluated through a large sample of events using the pseudo-code algorithm described in Appendix B.

B. Experimental Results

Experiment I: False Alarm Rates. In this experiment, we computed the FNR and FPR for IDS-1, IDS-2, and CKB/CIG. We used the pseudo-code to simulate $M = 10^2$ experiments of $N = 10^3$ attack/normal events. Fig. 8 shows the FNRs and Fig. 9 the FPRs (using box plots) for the attack rates $\hat{p}_0 \in \{0.25, 0.05\}$.

For the FNR case, the results show that for both $\hat{p}_0 = 0.25$ and $\hat{p}_0 = 0.05$, CKB/CIG outperforms IDS-2 but not IDS-1. This is because CKB and CIG label an event as an intrusion if and only if the event threatens the power grid. As a result, ineffective attacks are not labeled as intrusions, which increases the number of false negatives. If instead of computing the FNR for intrusions, we compute the FNR for threats (*i.e.*, FNR_t), then we will see how CKB and CIG outperform IDSs with no contextual information, which we describe in Experiment II.

For the FPR case, the results show that for $\hat{p}_0 = 0.25$, CKB/CIG performs worse than for IDS-1 and IDS-2. In a more friendly environment, *i.e.*, when $\hat{p}_0 = 0.05$, CKB/CIG outperforms IDS-1 but not IDS-2. This is because (i) the fast screening of CKB increases the number of false positives in a less friendly environment and (ii) CKB is sensitive to the number of critical targets (*i.e.*, the cardinality of L), which we describe in Experiment III.

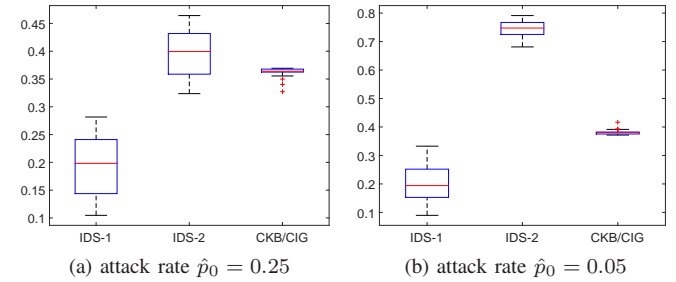


Fig. 8. FNR for IDS-1, IDS-2, and CKB/CIG

Experiment II: Threat Analysis. In this experiment, we computed the FNR for threats (*i.e.*, FNR_t). A false negative occurs if the random MCA was a threat for the power grid but CKB and CIG determined that it was not a threat. Fig. 10 shows the FNRs for the attack rates $\hat{p}_0 \in \{0.25, 0.1, 0.05\}$. As expected, the contextual information used by CKB and CIG considerably decreases the FNR for threats.

Experiment III: Sensitivity Analysis. In this experiment, we studied the sensitivity of FPR_t to the cardinality of L . Table I shows that the average FPR_t , denoted as $\mu(\text{FPR}_t)$, decreases as

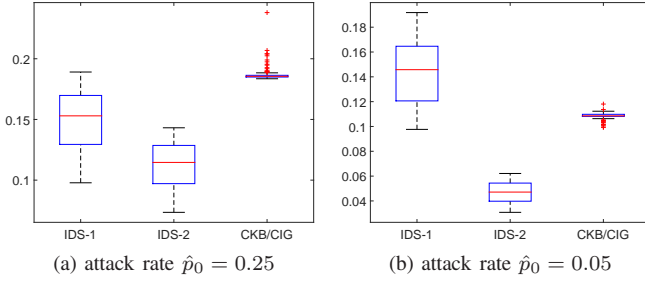
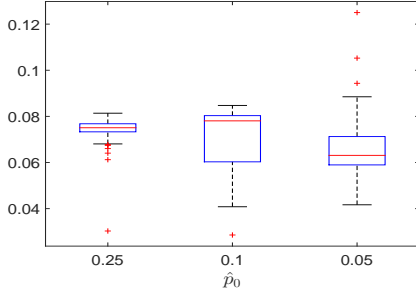


Fig. 9. FPR for IDS-1, IDS-2, and CKB/CIG

Fig. 10. FNR_t-Threat analysis.TABLE I
SENSITIVITY OF FPR_t.

| τ_l | L | $\mu(\text{FPR}_t)$ |
|----------|--|---------------------|
| 10 % | {3, 4, 13, 18, 25, 30, 42, 44, 45, 46} | 0.1806 |
| 20 % | {3, 4, 13, 18, 25, 30, 36, 42, 43, 44, 45, 46} | 0.1774 |
| 20 % | {3, 4, 25, 30, 45, 46} | 0.0625 |
| 30 % | {4, 13, 18, 25, 42, 45, 46} | 0.0646 |
| 30 % | {25, 46} | 0.0351 |
| 40 % | {13} | 0.0190 |

the number of critical/target lines decreases. This is because, as the number of critical lines decreases, the number of CI-tuples stored in CKB decreases too. As a result, the fast scanning feature of CKB will be less prone to false positives.

Note that there is a trade-off between the number of critical targets selected and the maximum FPR_t allowed, which should be adjusted based on risk assessment or experience. A different solution would be to always use CIG. This, however, will greatly increase the runtime of our proposed framework.

VII. CONCLUSION

In this paper, we developed a semantic analysis framework for Intrusion Detection Systems (IDS) against Monitor-Control Attacks (MCA) in power grids. The framework has two parts running in parallel with IDS: A Correlation Index Generator (CIG) that analyzes the correlation of potential hostile behaviors and indexes these behaviors, and a Correlation Knowledge-Base (CKB) that is updated with the Indices generated by CIG. The performance of the proposed framework is evaluated under different attack scenarios in a cyber-physical setting. It is shown that the proposed framework is capable of detecting MCA and estimating attack consequences with promising runtime and detection accuracy. In addition, the experiments show that the detection outcome of the proposed

framework is sensitive to both the size and locations of attack goals. Future work includes developing methods, which adapt CKB parameter settings to attack activities, to achieve an optimal trade-off between the FNR/FPR and detection runtime.

APPENDIX A PROOF OF PROPOSITION 1

Proof. Suppose, to get a contradiction, that $S' := S_{\alpha,j} \setminus \{s_k^*\}$ is an effective MCA. Thus, $S' \subset S_{\alpha,j}$ is a correlated MCA with cardinality $|S'| < |S_{\alpha,j}| =: \kappa^*$, which contradicts the fact that $S_{\alpha,j}$ is a strongly correlated MCA, *i.e.*, a CI with minimum cardinality. This proves the proposition. \square

APPENDIX B PSEUDO-CODE

We use Algorithm 1 to compute the FNR/FNR_t and FPR/FPR_t for CIG and CKB. Some remarks on Algorithm 1 are the following. (i) The if-conditionals describe how the E-blocks, CKB, and CIG interact during normal/attack events. (ii) Algorithm 1 describes attacks at the grid level, that is, either the grid is under attack $S_{\alpha,j}$ or not. We remark, however, that it can be easily adapted to model attacks at the substation level, that is, individual substations are under attack or not. (iii) Finally, by making the appropriate changes, Algorithm 1 can compute the FNR and FPR for IDS-1 and IDS-2.

Algorithm 1 Deriving FNR and FPR for CKB/CIG

```

1: (FNR, FPR) ← Rates()
2: procedure RATES()
3:   for  $k = 1$  to  $M$  do ▷ M: number of experiments
4:     for  $i = 1$  to  $N$  do ▷ N: number of attack/normal events
5:       Select  $p_1 \in [\hat{p}_0 - \delta, \hat{p}_0 + \delta]$ 
6:       Select  $p_2 \in [0, \beta]$ 
7:       Select  $p_3 \in [0, \alpha]$ 
8:       Attack( $i$ ) ← Bernoulli( $p_1$ ) ▷ Initiate attack/normal event
9:       if Attack( $i$ ) = 1 then ▷ Attack event
10:        [ $S_{\alpha,j}, \tilde{P}_d(a)$ ] ← RandomMCA
11:        ZD ← Bernoulli( $p_2$ ) ▷ ZD: zero-day attack
12:        Alarm ← Bernoulli( $\min\{1 - ZD, p_D\}$ )
13:        if Alarm = 1 then
14:          [Threat( $i$ ), isMCA] ← CKB( $S_{\alpha,j}$ )
15:          if isMCA = No then
16:            Threat( $i$ ) ← CIG( $S_{\alpha,j}, \tilde{P}_d(a)$ )
17:          end if
18:        else ▷ Zero-day attack case
19:          Threat( $i$ ) ← CIG( $\emptyset, \tilde{P}_d(a)$ )
20:        end if
21:      else ▷ Normal event
22:        FA ← Bernoulli( $p_3$ ) ▷ FA: false alarm
23:        Alarm ← Bernoulli( $\max\{FA, p_{FA}\}$ )
24:        if Alarm = 0 then
25:          Threat( $i$ ) ← CIG( $\emptyset, \tilde{P}_d$ )
26:        else ▷ False alarm case
27:          [ $S_{\alpha,j}, \tilde{P}_d$ ] ← RandomMCA
28:          [Threat( $i$ ), isMCA] ← CKB( $S_{\alpha,j}$ )
29:          if isMCA = No then
30:            Threat( $i$ ) ← CIG( $S_{\alpha,j}, \tilde{P}_d$ )
31:          end if
32:        end if
33:      end if
34:    end for
35:    FN, FP, TN, TP ← from Attack and Threat
36:    Compute FNR( $k$ ) and FPR( $k$ )
37:  end for
38:  return (FNR, FPR)
39: end procedure

```

REFERENCES

- [1] B. Zhu and S. Sastry, "Scada-specific intrusion detection/prevention systems: a survey and taxonomy," in *Proceedings of the 1st Workshop on Secure Control Systems (SCS)*, vol. 11, 2010.
- [2] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the ukrainian power grid," *SANS Industrial Control Systems*, 2016.
- [3] M. M. Hasan and H. T. Mouftah, "Optimal trust system placement in smart grid scada networks," *IEEE Access*, vol. 4, pp. 2907–2919, 2016.
- [4] D. Kuipers and M. Fabro, "Control systems cyber security: Defense in depth strategies," Idaho National Laboratory (INL), Tech. Rep., 2006.
- [5] J. Wang and C. Peng, "Analysis of time delay attacks against power grid stability," in *Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids*. ACM, 2017, pp. 67–72.
- [6] H. Lin, A. Slagell, Z. Kalbarczyk, P. Sauer, and R. Iyer, "Runtime semantic security analysis to detect and mitigate control-related attacks in power grids," *IEEE Transactions on Smart Grid*, 2016.
- [7] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 3104–3113, 2015.
- [8] C. Vellathurai, A. Srivastava, S. Zonouz, and R. Berthier, "Cpindex: cyber-physical vulnerability assessment for power-grid infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 566–575, 2015.
- [9] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580–591, 2014.
- [10] C.-C. Sun, J. Hong, and C.-C. Liu, "A coordinated cyber attack detection system (ccads) for multiple substations," in *Power Systems Computation Conference (PSCC), 2016*. Power Systems Computation Conference, 2016, pp. 1–7.
- [11] N. Liu, J. Zhang, H. Zhang, and W. Liu, "Security assessment for communication networks of power control systems using attack graph and mcdm," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1492–1500, 2010.
- [12] M. Vrakopoulou, P. M. Esfahani, K. Margellos, J. Lygeros, and G. Andersson, "Cyber-attacks in the automatic generation control," in *Cyber Physical Systems Approach to Smart Electric Power Grid*. Springer, 2015, pp. 303–328.
- [13] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for scada systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836–1846, 2008.
- [14] C.-W. Ten, A. Ginter, and R. Bulbul, "Cyber-based contingency analysis," *IEEE Transactions on Power Systems*, vol. 31, no. 4, pp. 3040–3050, 2016.
- [15] H. Song, R. Srinivasan, T. Sookoor, and S. Jeschke, *Smart Cities: Foundations, Principles, and Applications*. John Wiley & Sons, 2017.
- [16] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 226–231.
- [17] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3864–3872, 2016.
- [18] J. Wang and C. Moya, "Attack path reconstruction from adverse consequences on power grids with a focus on monitoring-layer attacks," in *Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG), Joint Workshop on*. IEEE, 2016, pp. 1–6.
- [19] C. Moya, C. Sun, J. Wang, and C. Liu, "Defending against measurement attacks on sub-transmission level," in *Power Energy Society General Meeting, Boston*, 2016.
- [20] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, E. G. Im, B. Pranggono, and H. Wang, "Multiattribute scada-specific intrusion detection system for power networks," *IEEE Transactions on Power Delivery*, vol. 29, no. 3, pp. 1092–1102, 2014.
- [21] C.-C. Liu, C.-W. Ten, and M. Govindarasu, "Cybersecurity of scada systems: Vulnerability assessment and mitigation," in *2009 IEEE/PES Power Systems Conference and Exposition*, 2009.
- [22] C.-W. Ten, C.-C. Liu, and M. Govindarasu, "Vulnerability assessment of cybersecurity for scada systems using attack trees," in *Power Engineering Society General Meeting, 2007. IEEE*. IEEE, 2007, pp. 1–8.
- [23] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.
- [24] X. Liu and Z. Li, "False data attacks against ac state estimation with incomplete network information."
- [25] J. Liang, O. Kosut, and L. Sankar, "Cyber attacks on ac state estimation: Unobservability and physical consequences," in *PES General Meeting—Conference & Exposition, 2014 IEEE*. IEEE, 2014, pp. 1–5.
- [26] C. Kahn, P. A. Porras, S. Staniford-Chen, and B. Tung, "A common intrusion detection framework," 1998.
- [27] H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems," *Computer Networks*, vol. 31, no. 8, pp. 805–822, 1999.
- [28] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," Technical report, Tech. Rep., 2000.
- [29] F. Dorfler and F. Bullo, "Novel insights into lossless ac and dc power flow," in *Power and Energy Society General Meeting (PES), 2013 IEEE*. IEEE, 2013, pp. 1–5.
- [30] C. Moya and J. Wang, "Developing correlation indices to identify coordinated cyber-attacks on power grids," *CoRR*, vol. abs/1707.00672, 2017. [Online]. Available: <http://arxiv.org/abs/1707.00672>
- [31] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on power systems*, vol. 26, no. 1, pp. 12–19, 2011.
- [32] A. A. Cárdenas, J. S. Baras, and K. Seamon, "A framework for the evaluation of intrusion detection systems," in *Security and Privacy, 2006 IEEE Symposium on*. IEEE, 2006, pp. 15–pp.
- [33] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," <http://cvxr.com/cvx>, Mar. 2014.