Cross-Layer Security Framework for Smart Grid: Physical Security Layer

Mohammed M. Farag[§], Mohamed Azab[*], Bassem Mokhtar[§]
[§]Electrical Engineering Department, Faculty of Engineering, Alexandria University, Alexandria, Egypt
{mmorsy, bmokhtar}@alexu.edu.eg
[*]The City of Scientific Research and Technological Applications, Alexandria, Egypt
mazab@vt.edu

***Abstract*—Security is a major challenge preventing wide deployment of the smart grid technology. Typically, the classical power grid is protected with a set of isolated security tools applied to individual grid components and layers ignoring their cross-layer interaction. Such an approach does not address the smart grid security requirements because usually intricate attacks are cross-layer exploiting multiple vulnerabilities at various grid layers and domains. We advance a conceptual layering model of the smart grid and a high-level overview of a security framework, termed CyNetPhy, towards enabling cross-layer security of the smart grid. CyNetPhy tightly integrates and coordinates between three interrelated, and highly cooperative real-time security systems crossing section various layers of the grid cyber and physical domains to simultaneously address the grid's operational and security requirements. In this article, we present in detail the physical security layer (PSL) in CyNetPhy. We describe an attack scenario raising the emerging hardware Trojan threat in process control systems (PCSes) and its novel PSL resolution leveraging the model predictive control principles. Initial simulation results illustrate the feasibility and effectiveness of the PSL.**

***Keywords*— Smart Grid, Smart Grid Security, Cross-Layer Security, Physical Layer Security, Process Control Security.**

I. Introduction

The smart grid is a cyber-physical system that tightly integrates control, computation, and communication technologies in the electrical power infrastructure. The smart grid has emerged as the next generation power grid aiming at enhancing the efficiency, reliability, and resilience of legacy power systems by employing information and communication technologies (ICT) [1]. To enable the smart grid global vision, widespread sensing and communication between all grid components is established via communication networks and managed by cyber systems. Extensive deployment of and reliance on ICT inevitably expose the smart grid to cyber security threats increasing the risk of compromising reliability and security of the electrical power infrastructure.

The scale and complexity of the smart grid create several vulnerabilities and provide numerous attack entry points. Therefore, security as a major challenge preventing wide deployment of this promising technology. Typically, the classical power grid is protected with a set of isolated and uncoordinated security tools applied to individual grid components and layers ignoring their cross-layer interaction. Such an approach does not address the smart grid security requirements. Usually, intricate attacks exploit multiple vulnerabilities of various grid systems and layers leveraging isolation and lack of awareness and cooperation between security tools protecting them.

Figure 1 depicts a conceptual hierarchical model of our development for the smart grid as a set of correlated interacting layers. At the top of the model is physical systems and devices participating in the generation, transmission, distribution, and consumption sectors of the grid. The physical domain is managed and operated by cyber systems and instruments that provide local control and computation capabilities required by the physical systems in addition to enabling inter- and intera-communication between the physical and cyber domains.

The physical domain is tightly coupled to the cyber domain via a grid network represented by a network layer encapsulating both data and control traffics. The smart grid network is an integration of (i) electric power grids that delivers electricity from power generation sources to end-users and (ii) effective two-way digital communication networks between utilities and consumers that monitors, manages, and controls the grid operations, renewable resources, and energy demands [2]. The cyber domain is represented by two sub-layers, the cyber or application sub-layer where the management and control logic resides, and the hardware sub-layer hosting such logic and providing the needed interfaces for data exchange. The high-level system management resides mainly in the upper two layers, the cyber layer where the management and control applications and software which are operated by a set of system operators and administrators. As depicted in the model, each layer is supported by a cyber layer comprising a set of hardware components and software systems.

Each layer in the presented model denotes a broad hierarchical model encapsulating interrelated sub-layers. For example the network layer in the smart grid model is a representation of the hierarchical OSI model. Usually existing security systems address security of a single layer or sub-layer in the hierarchical model neglecting security concerns of other layers and interaction between interrelated layers. However, the smart grid with its large scale, complexity, and importance is an easy target for cross-layer cyber attacks exploiting the lack of collaboration between security tools at different layers.

We advance an integrated security framework, termed CyNetPhy, supported by three main security layers, namely, the Cyber Security Layer (CSL), the Behavior Estimation Layer (BEL), and the Physical Security Layer (PSL) collaborating towards enhanced, cross-layer smart grid security. The CSL is mainly responsible for securing the cyber domain by supervising, managing, and coordinating between existing security tools. A set of smart distributed mobile agents pervasively crawls the grid's cyber domain to execute the CSL missions.

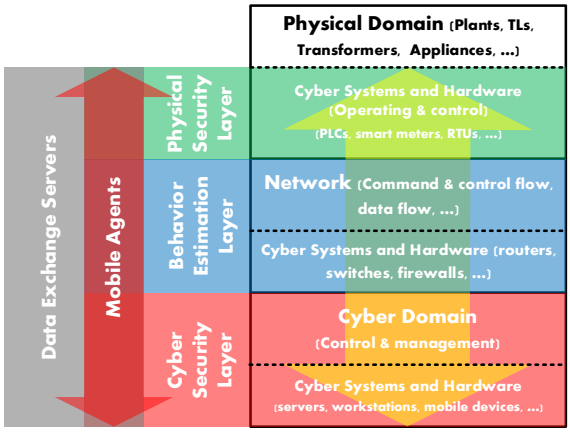

Fig. 1. Smart grid hierarchical model and layers interaction with CyNetPhy

The BEL monitors, analyzes and learns patterns of the grid network data and control flows independently to extract semantic feedback about behavior of various grid systems and layers. A set of distributed, autonomous, intelligent BE agents equipped with machine learning algorithms and intelligence techniques is employed to reason about semantics that can help in recognizing normal/abnormal behavior of various grid systems and components. The PSL is responsible for monitoring and protecting individual cyber systems with direct access to the physical domain. Security policies are derived from the system physical characteristics and component operational specifications, and translated into security monitors and components that can be implemented in either hardware- or software-based platforms. Hardware-based security is preferred due to the hardware immunity against software-based attacks and the superior performance offered by hardware [3]. A set of the CSL mobile agents is dedicated to enabling cross-layer interaction between the three security layers in real-time.

In this article we present an overview of the CyNetPhy security framework with emphasis on the PSL. Particularly, we focus on process control systems (PCSes) as an important part of the smart grid and as a clear example demonstrating our approach to secure the physical layer. More specifically, we advance a novel approach leveraging the model predictive control principles to secure PCSes vulnerable to the hardware Trojan threat. The remaining of this paper is organized as follows: Related security solutions for PCSes are presented in Section II. A high-level overview of the CyNetPhy framework is introduced in Section III. More technical depth for the PSL is advanced in Section IV. The PSL Trojan resolution method in PCSes is presented in IV-A, and preliminary simulation results of the security system developed for an automatic voltage regulator (AVR) PCS are presented in Section IV-B. Conclusions and future work are portrayed in Section V.

II. Background

Cyber attacks against the smart grid exploits the cyber domain as an easy access point to launch sophisticated attacks targeting the physical domain either indirectly by compromising the cyber and network domains, or directly by corrupting cyber systems controlling the physical domain [4]. Liu *et al.* presented an overview of relevant cyber security and privacy issues in smart grids [5]. Every aspect related to the cyber technology in the smart grid has potential vulnerabilities due to inherent security risks in the classical cyber environment. Interacting with the physical world shifts these vulnerabilities from the cyber to the physical domain. Current smart grid security systems lack for real-time situation awareness and cooperation between grid's components and defense tools. This isolation has serious impact not only on the operational aspects of the grid, but also on the security and safety aspects.

Recent attacks against power systems such as Stuxnet highlight vulnerabilities and the inadequacy of existing security systems. The Stuxnet worm infects the cyber domain, spreads via networks and removable storage devices, and exploits four zero-day attacks to manipulate the physical equipment. The primary target is believed to be an Iranian nuclear power plant, and likely caused a 15% drop in production of highly enriched uranium [6]. Defense against such complex attacks requires coordination and collaboration between various security systems crossing different layers to address the grid security concerns.

Attacks against the cyber layer operating the physical systems have a serious impact to security because of its direct interaction with the physical domain. Usually cyber attacks against this layer aim at disrupting the underlying physical systems by compromising the operation of the cyber components. PCSes are a typical example of security-critical cyber systems with direct access to the physical domain. PCSes are automatic feedback control systems where an embedded controller uses sensor measurements of a physical plant to compute feedback signals preserving system stability. Due to their importance in the power grid and their connection to national security, PCSes are exposed to a growing number of attacks [7]. PCSes are usually built using untrusted components and rely on perimeter security defenses rendering them vulnerable to insider threats and intricate outsider attacks. Recent attacks against PCSes such as Stuxnet have highlighted the inherent vulnerabilities and the inadequacy of existing security solutions [6].

Typically, security defenses in PCSes monitor either the controlled physical plant or the embedded PCS to detect behavior deviation from reference specifications. Sha introduced a protection method based on monitoring physical process measurements to detect faults [8] as illustrated in Figure 2(a). Dai *et al.* advanced a fault detection scheme based on observing PCS responses to new sensor inputs [9] as shown in Figure 2(b). Cárdenas *et al.* presented a physical model-based attack detection method complementing intrusion detection methods for networks and computer systems [10] as depicted in Figure 2(c). Unfortunately, these approaches are reactive and can only detect erroneous PCS behavior after its occurrence which might allow the controlled physical system to become unstable before adequate countermeasures can be applied.

III. CyNetPhy Security Framework

We present a three-layer framework, called CyNetPhy, with a cross-layer distributed, smart, real-time defenses to simultaneously address security of the cyber, network, and physical domains against pervasive and persistent attacks. The individual defense systems address the major concerns of smart grid security and collaborate together with autonomous management and coordination to enable prompt detection of well-known and zero-day cyber attacks. The security framework fills the gap between research and practice by advancing an

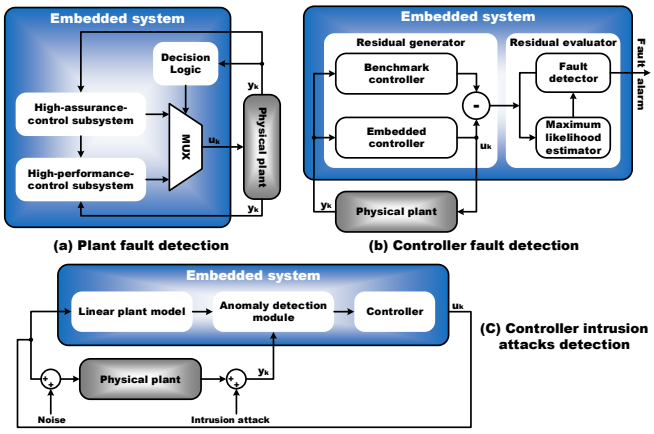

Fig. 2. Related cyber security approaches in PCSes [8]–[10].

integrated solution addressing security at different layers and domains rather than just addressing a single aspect or layer.

The CyNetPhy framework has three phases of operation: real-time monitoring, anomalous event investigation, and proactive actuation. In the monitoring phase, the three security systems monitor and analyze real-time data and operation of the underlying protected layers and forward abstract reports to the BEL to be analyzed at a higher abstraction level. Upon detecting anomalous or malicious behavior, the concerned layer initiates the investigation phase where the three security layers exchange relevant data to ascertain about the event and initiate the resolution procedures. In the actuation phase, the concerned layer applies a set of countermeasures to resolve confirmed security incidents such as raising alarms to system operators, isolating suspect systems, and finding suitable alternatives.

The first layer of CyNetPhy, termed CSL, works mainly on the cyber domain and cooperates with the other two layers to achieve its designated objectives. The CSL enables Monitoring, Analysis, Sharing, and Control (MASC) technology to ensure effective smart grid security. Most current technologies did not consider that cyber and physical convergence would need a new paradigm treating cyber and physical components seamlessly. Furthermore, information sharing was severely curtailed by enforcing perimeter defenses to preserve privacy of the smart grid. These limitations negatively impact quality, reliability, survivability, and promptness of security services.

The CSL is an evolution of the cyber MASC framework CyMASC presented in [11] towards realizing pervasive MASC for enhanced smart grid security. The CSL is an intrinsically-resilient, situation-aware system that intelligently manages the existing security tools to provide evolutionary security services. The CSL intelligently mixes and matches heterogeneous tools and control logic from various sources towards dynamic security missions. The CSL is also elastic where situation-driven MASC solutions can be dispatched using dynamic sets of mobile agents circulating the smart grid network rather than using pre-deployed components. Such an approach provides evolvable, pervasive and scalable MASC services.

The CSL circulates context-driven, functionally customizable mobile agents into the smart grid body to pervasively monitor, analyze and control those components. A mobile agent is a composition of computer software and data encapsulated in a migratable (movable) format. Mobile agents leverage one of the "write once, run anywhere" (WORA) languages like Java, or C# to build a partially compiled code that can run on any host machine with the needed libraries installed. Mobile agents autonomously move from one computer to another in the network to execute a certain mission. The mobility feature of mobile agents enables them to travel in the smart grid network and carry relevant data along with them. We securely design the agents to hide and protect security-relevant information. Due to reliance on several mobile agents rather than static tools, security of the smart grid is not vulnerable to a single point of failure, and the CSL protection can continue even if individual nodes fail or become unavailable

The main functionality of the CSL mobile agents is to execute defense missions provisioned by the grid operator and defense service provider. A defense mission is composed of a set of sensing and affecting tasks involving information gathering, partial analysis, control, and manipulation of the grid components. Due to their mobility feature, the CSL mobile agents are responsible for inter-layer communication and data exchange tasks in the CyNetPhy framework. The CSL utilizes such pervasive activities to build real-time global views of the entire grid reflecting the quality of the security service and the current state at each point. These views are intelligently analyzed to facilitate evolution of security services [12].

The hierarchical structure of the CSL sensing and affecting framework is composed of three main layers: management layer, sensing and affecting abstraction layer, and the defense delivery tools. The sensing and affecting tool layer is a set of logical sensing or affecting APIs stored in the machine local libraries. These tools are autonomously abstracted at run-time into uniform sensing and affecting agents participating in the creation of a cooperating agent group conducting specific defense missions. The CSL agent groups are anonymously constructed, managed, and controlled at run-time by the CSL management layer, which is also responsible for collecting, correlating, and analyzing sensor feedback data.

In addition to the smart utilization of the mobile agents in provisioning on-demand conventional defense services to the cyber hosts, the CSL collects host-oriented real-time feedback from its agents investigating various aspects that might be an indication of malicious behavior evading detection by existing security tools. The CSL alternates/mixes different security/control missions from different sources to provide security services to the same grid host. This procedure involves sharing security experience and tools between hosts. Shared materials are autonomously checked for privacy violations before utilization or storage. The CSL enables the security tools in the grid's cyber domain to continuously evolve their services and capabilities that can lead to more accurate and prompt detection of known attacks and better chance in detecting zero-day attacks. This layer is also responsible for decision making based on the sensing feedback, previous historical events, and CyNetPhy security guidelines. Such decisions might involve composing more capable affecting defense missions for resolution or new sensing missions for deeper investigation [12].

The second layer of CyNetPhy, termed BEL, is mainly concerned with behavior awareness of the smart grid via analyzing and learning patterns indicating normal/abnormal behavior of different grid systems and components. We hypothesize that grid measurement data exhibits multi-dimensional patterns that

can be learned to extract data features and semantics. Such patterns can reveal precious information about the grid security state. The BEL operation relies on i) collecting raw data concerning the smart grid from the network data and control traffic flows; and ii) learning patterns of captured data to extract a group of features and reason about semantics. The BEL is the intelligent part of CyNetPhy that has the ability to read between the lines and initiate proactive measures to preempt potential cyber threats in collaboration with the PSL and CSL.

The Behavior learning process conducted by the BEL involves a set of learning and evolution operations. The BEL captures raw data from the power and information flows in the smart grid. This data is represented as attribute-value pairs using specific data representation models. Then, the BEL employs classification techniques in order to classify extracted attributes based on their values. Each set of classified attributes related to a specific grid component, layer, or domain are fed into behavior semantics reasoning models implemented using monolithic or hybrid intelligence techniques such as Hidden Markov Model (HMM). Operation parameters of reasoning models are designed and refined based on historical data, which are used for training the models in a supervised or an unsupervised way. According to the input group of attributes to reasoning models and attributes' values, the models will extract correlated semantic topics which can characterize behavior of various grid components at different levels of granularity.

A set of distributed, autonomous, intelligent BE agents is implemented over secure, high-performance servers and equipped with machine learning algorithms and intelligence techniques to reason about semantics that can help in recognizing normal/abnormal behavior of various grid elements. The BE agents use a set of distributed dynamic reasoning models in order to fine-granulate semantics extraction processes and build efficient dynamic behavior models regarding normal/abnormal behavior of diverse grid components. Due to the complexity and scalability of the smart grid, the BE agents are distributed and managed in a hierarchical fashion. A set of agents inspects behavior of a particular part of the grid according to specific criteria and sends abstract reports to higher hierarchical agents.

The BE agents also utilize data profiling and dimensionality reduction techniques to reduce dimensions of large-scale, high-dimensional measurement data and to find similarities among these data. Such an approach enables development of resource-efficient agents and helps in mitigating the problem of "data tsunami" [13] arising due to the massive amount of data collected by high-frequency data measurement units. Semantic reasoning techniques of our development will be able to work over reduced-dimensional data. In our previous work, we presented a network memory management system for semantics extraction services which can be implemented over the BE agents to enable the BEL operations and goals [14].

For the AVR control system case study presented in this paper, the BE agents will employ HMM for learning and classifying behavior of running AVRs in a power system. The HMM operation relies on a set of attribute-value profiles represented by agents in their internal memories, according to the raw data collected from the power and information flows in the power generator. A profile might comprises attributes such as "input voltage level", "output voltage level", "load type" and "line regulation". Based on the HMM parameters, training using historical data, and values of the selected attributes, HMM outputs the most likelihood observations which are stored as interrelated semantics for AVR behavior. For example, a learned AVR semantic topic might be "normal AVR behavior in residential load includes good line regulation".

The third layer of CyNetPhy, termed PSL, is mainly concerned with security of individual systems and components operating the physical layer in the grid. Direct interaction with the physical domain is a featured property of this layer distinguishing it from other smart grid layers. The physical layer comprises a set of application-specific embedded systems and devices with clearly defined functionalities and objectives. Smart meters, Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), and PCSes are typical examples of the units protected by the PSL. Usually cyber attacks against this layer aim at misleading the upper layers of the grid or disrupting the underlying physical systems by compromising the operating cyber components. Clarity of objectives for both the physical layer and the associated cyber threats enables framing security policies and specifications capturing secure and trusted operation of the protected systems. The PSL collaborates with the BEL and CSL by exchanging relevant data, delivering accurate measurements about particular cyber systems, and applying adequate countermeasures in the physical domain. In the next section we detail the PSL and advance an attack scenario against a PCS of a power plant and its PSL resolution.

IV. Physical Security Layer

Typical system behavior and specific security checks are derived from the system physical characteristics and models and component operational specifications, and translated into hardware guards and wrappers to enable persistent monitoring and verification of the protected systems at run-time. Proliferation of hardware attacks and their direct impact to the cyber and physical domains is the main motivation to consider hardware-based security. The PSL security components are synthesized in reconfigurable hardware to meet various objectives, including: improved security of hardware defenses, immunity against software-based attacks, the ability to detect insider and hardware-based threats, superior hardware performance, and the flexibility provided by reconfigurable hardware. Custom-designed hardware monitors and wrappers are attached to input and output (I/O) interfaces of the system under protection with the main goal of detecting malicious and anomalous activities associated with potential cyber attacks in real-time. The PSL security components are an evolution and a direct application of the predictive security system presented in [15] towards protecting PCSes in the smart grid.

In addition to their real-time monitoring role, hardware security components will act as trust anchors—independent monitoring and control devices with access to the system interfaces and inner components—for the protected systems. Chavez presents the concept of trust anchors to protect PCSes against lifecycle attacks in [16]. Trust anchors can provide unbiased measurements at the lowest level of a system (the hardware-level) that independently verify system operation, reveal deceptive malicious behavior, independently attest to system state, and verify the correctness of system tests. They also offer unimpeded control that makes it possible to implement trusted control functions, remove discovered malicious content,

execute system tests, and analyze suspected system compromise [17]. Trust anchors are the PSL components responsible for interacting with the CSL and BEL. Specific security actions can be initiated based on issued requests including measuring physical quantities, applying specific checks, reporting events and raising alarms to the upper layers, applying a recovery strategy, and switching to local or remote backup systems.

A. Model Predictive Security of Process Control Systems

A PCS is an embedded platform realizing automatic feedback control for physical processes. PCSes are often assembled from untrusted components provided by the global supply chain. Trojan horses are emerging threats with malicious intentions that can be introduced into an embedded system design as either hardware or software modifications to the system implementation during different phases of the system's lifecycle. Trojans are difficult to detect using conventional pre-deployment verification techniques and perimeter security defenses, and their effects to the host platform range from subtle disturbances to complete system failures. We present a novel approach to predict and preempt Trojan threats in PCSes as an example of PSL treatment of potential cyber threats in the physical domain. More specifically an AVR PCS, which keeps the voltage level constant at rated value in power generators, demonstrates the Trojan and PSL resolution.

The threat model assumes a Trojan-infected PCS supplied by an untrusted supply chain and controls a security-critical physical system. The Trojan is detected using neither perimeter security tools nor pre-deployment verification and Trojan detection methods. The Trojan is kept dormant and is activated upon occurrence of a rare triggering condition or after passing a specific period of operation (time-bomb). The Trojan payload aims at compromising the PCS functionality to rapidly push the controlled physical process out of its stability conditions. Such an attack cannot be detected in the nick of time using classical reactive security systems that might allow the physical process under control to become unstable before corrective actions can be applied. Fortunately, the PSL employs a proactive approach that enables detecting and preempting Trojan threats.

The PSL acts as a last-line-of-defense against cyber threats with the main objective of providing prompt measures in collaboration with the BEL and CSL to protect the physical domain, particularly PCSes, from threats evading detection by design-time verification methods and perimeter security defenses. This objective can be achieved by identifying such threats ahead of time before affecting the physical domain, or in other words by predicting them. The main idea to predict the Trojan threats is to emulate the control process at run-time in an accelerated-time manner to give a short-term projection of future PCS actions. To achieve this, an accelerated model of the physical process is controlled by an identical instance of the PCS which will be subject to the same operating conditions. To maintain convergence with the physical plant, the model's state is periodically synchronized with the physical plant's estimated state. The accelerated control system is monitored to foresee erroneous controller behavior. For the physical domain, specifications for normal system behavior are already known and precise models of physical processes usually exist. Such specifications and models are used to implement the security monitors in hardware. Once a cyber threat is detected in the accelerated control system, a preemptive measure can be applied such as switching the operating PCS to a backup one.

This approach exploits the operation speed variance between a physical process and its model, which is analogous to the difference between running and simulating the physical process. The idea of using an accelerated accurate model to predict controller behavior is known as Model Predictive Control (MPC) in the automatic control literature [18]. The main objective of MPC is to control a multiple-input multiple-output (MIMO) process while satisfying inequality constraints on the input and output variables. In this work, we advance a Model Predictive Security system (MPS) and use it differently to predict future controller actions, detect erroneous behavior, and preempt consequences to the physical system.

Figure 3 depicts the high-level architecture of the MPS to predict Trojan threats in PCSes developed for a general feedback control system. Basic components of the MPS are:

- The operating control system containing a PCS embedded controller, a distinct backup controller, a switching circuit, and a state estimator. This system runs at the typical sampling rate of the physical plant.
- The accelerated MPC system containing an accelerated state-space plant model implemented on an embedded system, and an identical instance of the PCS controller. This system runs n times faster than the operating control system.
- The PSL security modules including an interface guard for the operating control system and a monitoring module for the accelerated control system.
- A state synchronization switch and timing modules for clock generation and time management.

The security monitor module observes the accelerated MPC system to check the PCS operation compliance to the PSL security specifications. Detection of abnormal behavior in the accelerated MPC system triggers the interface guard in the operating control system to switch the operating controller to the backup one and raise an alarm to the BEL via the CSL mobile agents. The synchronization module is responsible for periodically updating the model's state with the estimated state of the physical process. A sample and hold module periodically updates the accelerated MPC system's input with the physical plant's reference input. The timing module is responsible for clock generation and time management for the whole system. For further details about the concepts, organization, and time management in the MPS we recommend reading [15].

B. Evaluation and Results

In order to clarify and evaluate the MPS role in the PSL, an AVR excitation controller of a synchronous power generator is presented as a case study. The main objective of power system operation and control is to maintain a continuous supply of power with an acceptable quality and voltage profile. AVRs are cost-efficient PCSes widely deployed in power generators [19]. The excitation system maintains the generator voltage and controls the reactive power flow using an AVR keeping the voltage magnitude of a generator at a rated value. Thus, cyber attacks targeting the AVR PCS can directly ruin the controlled power generator and indirectly deteriorate reliability and efficiency of the smart grid . Nevertheless, the MPS can be generally applied to other physical systems in the smart grid.

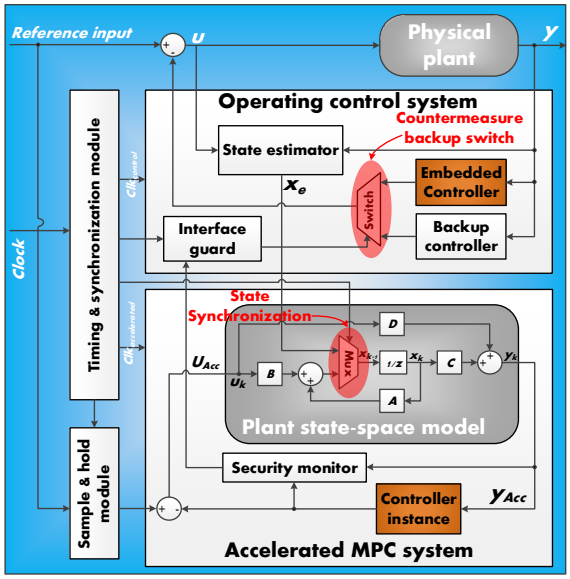

Fig. 3. High-level architecture of the MPS

Figure 4(a) depicts a one-line diagram of the open-loop power system, including a synchronous generator, exciter, amplifier, and a sensor, and their I/O transfer functions. The physical parameters of the amplifier, exciter, and generator shown in Table I are provided by [19]. Figure 4(b) shows a block diagram of the feed-forward digital PID controller. The discrete-time PID controller is developed in the parallel form with forward Euler integration and filtering methods, and have the following transfer function:

$$G(z) = K_p + K_i T_s \frac{1}{z-1} + K_d \frac{N}{1 + N T_s \frac{1}{z-1}} \qquad (1)$$

Figure 4(c) depicts a block diagram of the generator state-feedback controller realized using the linear-quadratic regulator (LQR) optimal control technique [20]. LQR controllers are widely deployed, and their structure helps to present our concepts and architecture effectively, nevertheless, our approach is still applicable to other control techniques. The main control objectives are preserving system stability, minimizing the output error and control effort, and optimizing the transient response characteristics. The continuous-time state-space equation describing the generator is given by:

$$\dot{x} = Ax + Bu$$
$$y = Cx + Du$$

where $A = \begin{bmatrix} -13.5 & -4.688 & -1.563 \\ 8 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 4 \\ 0 \\ 0 \end{bmatrix}$, $C = [0 \quad 0 \quad 3.906]$, and $D = 0$.

To design the LQR state feedback controller, we define the state-cost weighted matrix $Q = pC^TC$, and the control weighted matrix $R = 1$, for simplicity. The weighting factor p is chosen by trial and error in order to tune the step response to achieve the control objectives. The control matrix K is calculated for the closed-loop poles satisfying the LQR optimization objectives, and the reference scaling precompensator gain $Nbar$ and the state observer gain L are calculated, accordingly. Table I shows the digital PID and LQR controller gains which are tuned and calculated using the Matlab control toolbox for a sampling time $T_s = 10$ msec.

TABLE I. PHYSICAL SYSTEM PARAMETERS AND CONTROLLER GAINS

System parameters				PID		Observer (L)	LQR (K)
K_a	10	T_a	0.1	K_p	0.1888	67.6962	2.0819
K_e	1	T_e	0.4	K_i	0.1842	21.0692	4.5902
K_g	1	T_g	1	K_d	0.0262	0.6196	11.4536
K_s	1	T_s	0.05	N	5.3815	$Nbar$=3.0333	

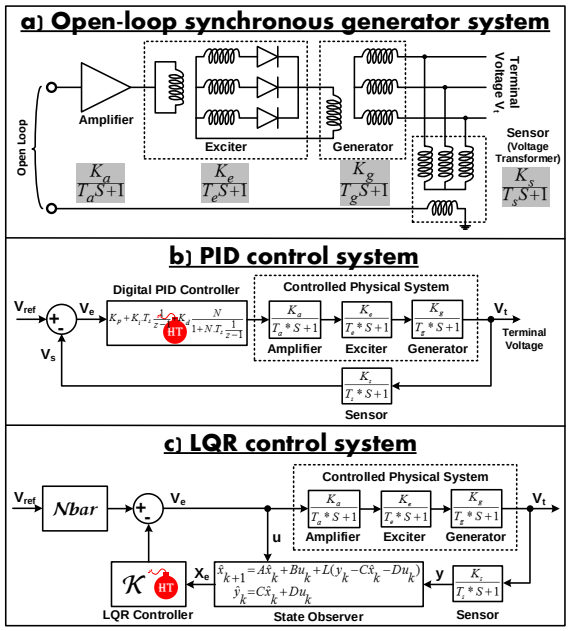

Fig. 4. Open-loop, PID, and LQR AVR controllers of a synchronous generator

We developed both time- and event-triggered Trojans and inserted them into the PID and LQR controllers, respectively. The time-triggered Trojan is kept dormant for a specific time duration and when activated it bypasses the PID controller by directly connecting its input and output. The event-triggered Trojan counts zero-crossing events in the state signals X_e and is activated at a specific count with a payload that changes the LQR controller gain K. For both Trojans, the payload aims at rapidly pushing the controlled generator out of its stability.

The MPS architecture shown in Figure 3 was modeled and simulated in Matlab Simulink for both classical (PID) and modern (LQR) PCSes. The accelerated MPC system sampling time T_s is 1 msec which is 10 times faster than the operating control system, resulting of a time scaling factor of $n = 10$. For the discrete-time accelerated MPC system, scaling down the sampling time of the plant model by a factor of n enables the system to run n times faster than the operating control system. Synchronization time T_{sync} between the accelerated model and estimated physical system states controls the time period of the foreseen controller actions, termed prediction window T_{pred}. A moving prediction window enables periodic projection of the future system state from the updated current system state. We developed the accelerated MPS for two different values of T_{sync}. The time scaling factor n and the T_{sync} are the two MPS independent design parameters, and T_{pred} is the dependent parameter, where $T_{pred} = nT_{sync}$. For more details about time management in the MPS we refer to [15].

Figure 5 depicts the regulated generator voltage and the MPS output for both the Trojan-free and Trojan-infected PID and LQR PCSes. As shown by Figure 5(a), the generator becomes stable after $T_{settling}$, and the LQR PCS has better

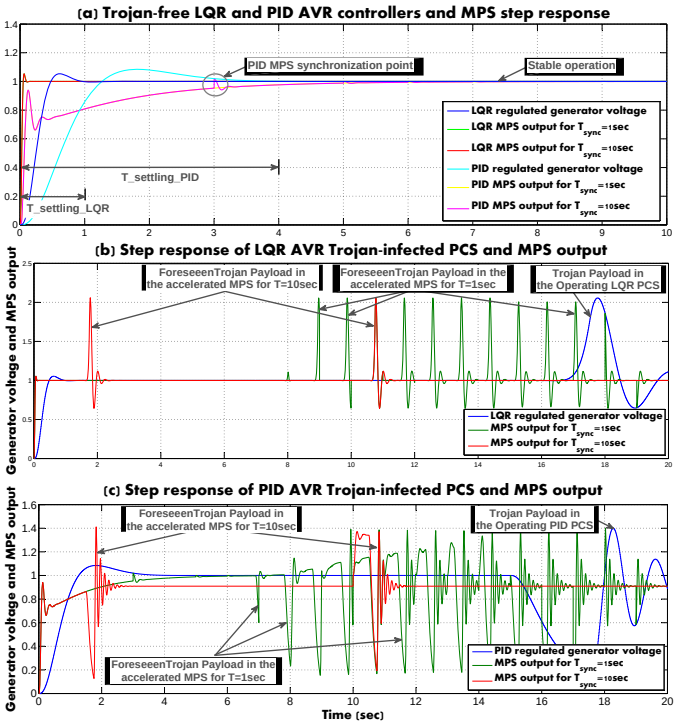

Fig. 5. Step response of Trojan-infected AVR PCSes and MPS output

transient response characteristics compared to the PID AVR. For both PCSes, the accelerated MPS foresees the operating PCS output, and its state is periodically synchronized with the plant's estimated state every T_{sync} to prevent state divergence. As shown by Figure 5(b), (c), the inserted Trojans are activated in the LQR and PID operating PCSes at $t = 15$ sec, and their payloads cause an abrupt change in the generator voltage which can instantaneously devastate it if not detected.

Figure 5(b), (c) shows the MPS output for $n = 10$ and, $T_{pred} = 1$, and 10 sec. As demonstrated by the figure, both MPSes with different prediction windows foresee the Trojan payload in the accelerated PCS ahead of time before its real occurrence in the operating PCS. The MPS with $T_{sync} = 10$ sec, the larger synchronization time, predicts the fault earlier than the other one due to its large prediction window size. This comes at the price of increasing T_{sync} that might allow for state divergence and consequently inaccurate prediction. The MPS with $T_{sync} = 1$ sec foresees the fault more frequently due to its small prediction window size. Once the Trojan is detected, a switching circuit immediately switches the control path to a backup controller, which must be a variant of the infected one to preserve stability of the physical system.

V. Conclusions

Cross-layer rather than isolated solutions are needed to increase smart grid awareness and secure it against dexterous cyber threats. We presented a brief outline of a cross-layer security framework that integrates three security systems mainly concerned with the cyber, network, and physical domains separately and elaborated on the PSL to protect the cyber systems having direct access to the physical domain. A novel MPS for PCSes was advanced and its applicability was established using modeling and simulation for an AVR PCS. The MPS can help the smart grid infrastructure withstand an emerging Trojan onslaught. Hardware realization and experimental testing of the MPS are under development. Once the realization is complete, we will be able to asses the overheads and practical applications of the MPS. The BEL, CSL, and the integrated CyNetPhy framework, in addition to other aspects and capabilities of the PSL will be extended in our upcoming work.

Acknowledgment

This work is supported by the SmartCI Research Center.

References

[1] Xu Li, Xiaohui Liang, Rongxing Lu, Xuemin Shen, Xiaodong Lin, and Haojin Zhu. Securing smart grid: cyber attacks, countermeasures, and challenges. *Communications Magazine, IEEE*, 50(8):38–45, 2012.

[2] Billion Electric Co. Ltd. http://www.smartgrid.com.tw/.

[3] Mohammed M Farag. *Architectural Enhancements to Increase Trust in Cyber-Physical Systems Containing Untrusted Software and Hardware*. PhD thesis, Virginia Polytechnic Institute and State University, 2012.

[4] Terry Fleury, Himanshu Khurana, and Von Welch. Towards a taxonomy of attacks against energy control systems. In *Critical Infrastructure Protection II*, pages 71–85. Springer, 2009.

[5] Jing Liu, Yang Xiao, Shuhui Li, Wei Liang, and CL Chen. Cyber security and privacy issues in smart grids. *Communications Surveys & Tutorials, IEEE*, 14(4):981–997, 2012.

[6] Thomas M Chen and Saeed Abu-Nimeh. Lessons from Stuxnet. *Computer*, 44(4):91–93, 2011.

[7] M. Brundle and M. Naedele. Security for process control systems: An overview. *Security Privacy, IEEE*, 6(6):24–29, Nov–Dec 2008.

[8] Lui Sha. Using simplicity to control complexity. *Software, IEEE*, 18(4):20–28, Jul–Aug 2001.

[9] C. Dai, S.H. Yang, and Liansheng Tan. An approach for controller fault detection. In *Fifth World Conference on Intelligent Control and Automation (WCICA)*, volume 2, pages 1637–1641, Jun 2004.

[10] Alvaro A. Cárdenas, Saurabh Amin, Zong-Syun Lin, Yu-Lun Huang, Chi-Yen Huang, and Shankar Sastry. Attacks against process control systems: risk assessment, detection, and response. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ASIACCS'11, pages 355–366, 2011.

[11] Mohamed Azab and Mohamed Eltoweissy. Bio-inspired evolutionary sensory system for cyber-physical system defense. In *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, pages 79–86. IEEE, 2012.

[12] Mohamed Azab and Mohamed Eltoweissy. Intrusion detection and prevention in cyber physical systems. *The State of the Art in Intrusion Prevention and Detection*, page 155, 2014.

[13] Yih-Fang Huang, Stefan Werner, Jing Huang, Neelabh Kashyap, and Vijay Gupta. State estimation in electric power grids: Meeting new challenges presented by the requirements of the future grid. *Signal Processing Magazine, IEEE*, 29(5):33–43, 2012.

[14] Bassem Mokhtar, Mohamed Eltoweissy, and Hesham El-Sayed. Network "memory" system for enhanced network services. In *9th International Conference on Innovations in Information Technology (IIT)*, pages 18–23, 2013, 2013.

[15] Lee W Lerner, Mohammed M Farag, and Cameron D Patterson. Runtime prediction and preemption of configuration attacks on embedded process controllers. In *Proceedings of the First International Conference on Security of Internet of Things*, pages 135–144. ACM, 2012.

[16] Adrian R Chavez. Position paper: Protecting process control systems against lifecycle attacks using trust anchors.

[17] U.S. Department of Energy. http://cms.doe.gov/.

[18] Eduardo F Camacho and Carlos Bordons Alba. *Model predictive control*. Springer, 2013.

[19] H Shayeghi and J Dadashpour. Anarchic society optimization based PID control of an automatic voltage regulator (AVR) system. *Electrical and Electronic Engineering*, 2(4):199–207, 2012.

[20] K Ibraheem. A digital-based optimal AVR design of synchronous generator exciter using LQR technique. *Al-Khwarizmi Engineering Journal*, 7(1):82–94, 2011.