Title

A Hybrid Network IDS for Protective Digital Relays in the Power Transmission Grid

Authors

Koutsandria, Georgia
Muthukumar, Vishak
Parvania, Masood
et al.

Publication Date

2014-11-03

Peer reviewed

A Hybrid Network IDS for Protective Digital Relays in the Power Transmission Grid

Georgia Koutsandria*, Vishak Muthukumar†, Masood Parvania*, Sean Peisert†‡,
Chuck McParland‡, and Anna Scaglione*

*Department of Electrical and Computer Engineering, University of California, Davis, CA, USA
†Department of Computer Science, University of California, Davis, CA, USA
‡Lawrence Berkeley National Laboratory, Berkeley, CA, USA

***Abstract*—In this paper, we propose a novel use of network intrusion detection systems (NIDSs) tailored to detect attacks against networks that support hybrid controllers that implement power grid protection schemes. In our approach, we implement specification-based intrusion detection signatures based on the execution of the hybrid automata that specify the communication rules and physical limits that the system should obey. To validate our idea, we developed an experimental framework consisting of a simulation of the physical system and an emulation of the master controller, which serves as the digital relay that implements the protection mechanism. Our Hybrid Control NIDS (HC-NIDS) continuously monitors and analyzes the network traffic exchanged within the physical system. It identifies traffic that deviates from the expected communication pattern or physical limitations, which could place the system in an unsafe mode of operation. Our experimental analysis demonstrates that our approach is able to detect a diverse range of attack scenarios aimed at compromising the physical process by leveraging information about the physical part of the power system.**

I. Introduction

A. Scope and Goal

Industrial Control Systems (ICSs), such as those in the power grid, including "Supervisory and Data Acquisition (SCADA)" systems, constitute the fundamental elements in the operation of modern power systems, providing a wide range of applications that range from applications in large control centers to substations and control of individual components. While originally ICSs had minimal networking capabilities—generally a few serial ports per device—over the years, they have incorporated Ethernet modems and packet switched communications, to support communications with a large number of devices from a variety of vendors.

Despite the value proposition of the emerging smart grid, given that Ethernet communications can be exposed to traffic from a wide variety of sources [1], the ICSs that control critical physical power equipment on the grid are clearly also vulnerable to attack and manipulation over computer networks [2]–[4]. Therefore, given the potential impact that could result if such systems were compromised, securing networked ICSs is of high importance. Numerous traditional security countermeasures, such as firewalls, encryption, and network intrusion detection systems (NIDSs) [5], have been adopted to protect and isolate the network perimeter of many industrial control facilities from external attacks. However, these traditional security mechanisms have proven inadequate protection mechanisms. To further close this security gap for ICSs, we use an approach that builds on the operation of the physical systems themselves.

We build on the body of work on *hybrid control*, which models and studies mathematically the dynamic behavior of ICSs and other cyber-physical systems, representing them through, for example, hybrid automata models [6]. Such models capture both discrete and continuous aspects of the system behavior. In particular, power systems are characterized by a set of physical conservation laws (Kirchhoff's and Ohm's laws, electric motor dynamics etc.) and operational constraints (thermal or generation capacity, ramping etc.) that define the system's safe operational region, and must be enforced in order to guarantee reliable operation. Power systems use protection mechanisms (nowadays mostly digitally controlled) that follow specific hybrid automata models derived from such laws and operational limits. The ANSI/IEEE C37.2 standard [7] provides a taxonomy of these codified elements that are typically called interchangeably devices or functions. Various protection schemes are applied to power systems to ensure their safety, and decide about the state of the system, i.e., whether the system is under a safe or unsafe operation mode. Our basic tenet in this paper is that *both* the cyber and the physical context of the information exchanged in the control network can be used to check whether the system is consistent with the hybrid automata architectures.

Our goal is to translate this notion into what we call Hybrid Control Network Intrusion Detection Systems (HC-NIDS), which refers to a systematic approach to generate specification-based intrusion detection rules for control environments that make use of micro-processor based controllers and packet-switched communications. We demonstrate our approach by focusing in particular on protective digital relays in power systems and creating and testing rules that are a direct byproduct of the hybrid automata executed by the network of relays. Our novel use of NIDS integrates the computer and network security communication rules used by traditional NIDS approaches, with information related to the physical limits of the system, and the expected execution of its hybrid automata models, in order to mitigate an essential category of cyber-physical vulnerabilities.

B. Related Work and Contribution

Recent research on security for cyber-physical systems in the power systems field has been focused on re-applying traditional computer security mechanisms, such as encryption, firewalls, and IDSs. Numerous network intrusion detection

approaches for cyber-physical systems have been studied, proposed, and built [8]. *Misuse-based intrusion detection* is a technique that looks for "known bad" things. Morris, et al. [9], use this technique by introducing a number of misuse signatures for Modbus. This approach is effective for monitoring adherence to key protocol requirements and whether Modbus protocol communication rules are satisfied. However, it focuses on a generic approach related to the specifications of the protocols rather than distinct devices.

Anomaly-based intrusion detection is used to detect events that deviate from normal behavior by classifying them as normal or abnormal using statistical models. Historically, anomaly detection has not been very effective in IP networks and general-purpose computing because of high false positive rates, lack of "malicious" training data, and the lack of actionability of the alerts given [10]. These challenges are partially due to the fact that traffic on many IT networks is "noisy" and malicious activity often does not rise above the level of the noise of "normal" activity. It is also difficult to separate "abnormal but benign" activity from malicious activity.

Carcano, et al. [11], focused on attacks that appear legitimate when considered alone but can harm the system when combined with other actions. The approach focuses on the system's state by using the knowledge of the expected operation of a process, however, the scope of the process being considered does not extend to physical constraints and laws that should be satisfied to ensure stability of the system. *Specification-based* intrusion detection is the opposite of *misuse-based* detection, in that it looks for deviations from "known good" things. Berthier and Sanders [12] developed a specification-based monitoring system for smart meters by deploying an IDS sensor in the field to identify threats in real time. The sensor monitors traffic between smart meters and the utility network to ensure that devices are in a secure state and to prevent energy theft. In our work, we also use a specification-based approach, but we analyze the data with a different purpose in mind.

Cárdenas, et al. [13], examined SCADA vulnerabilities and presented a theoretical approach to control systems' security, performing linear feedback control for linear state space equations. This work is close to our approach with the difference that we focus on real automation applications typically met on power systems, that typically check the conservation of physical limits and laws that designate the stability.

In our earlier work [14], we presented a *hybrid control NIDS (HC-NIDS)* for automated power distribution systems, where we focused on the "fault location, isolation, and service restoration (FLISR)" process. In this paper, our case study is a typical protection mechanism implemented through digital relays used in the power transmission grid. Protective digital relays are typically used in power systems to perform automated control actions designed to protect physical equipment and ensure the stability of the system. Typically they help detect and isolate faulted sections from the rest of the transmission grid by continuously executing the same set of functions based on the system's physical limitations. Using the *overcurrent protection* scheme for a power transformer as an example, we discuss the HC-NIDS rule design approach, in a way that can be easily generalized to arbitrary control environments that include packet-switching technology (with the OSI communications protocol stack) to connect in a network micro-controllers that execute code and directly or indirectly interact with the physical machinery. Another contribution of our approach lies in the validation technique. Our experimental framework includes virtual physical models, created using the Simulink simulation environment, interacting with real and simulated embedded controllers (two Siemens Programmable Logic Controllers SIMATIC S7-1200 CPU 1212C AC/DC/RLY) to generate real network traffic that the HC-NIDS continuously monitors. To analyze the traffic and validate the viability of the HC-NIDS approach, we implemented our "hybrid" set of specification-based IDS rules, representing permissive device actions, as signatures for the popular Bro Network Security Monitor [15]. This experimental testbed allowed us to test the practical feasibility of our approach by emulating real cyber attacks that could occur on typical *overcurrent protection* schemes for a power transformers.

The remainder of the paper is organized as follows: Section II introduces the major components of the power grid, and presents several key security threats against power transmission systems. Section III presents our HC-NIDS approach, and the protection scheme that we use to validate the approach, including its hybrid automaton. The threat model is presented in Section IV, where we describe the attack scenarios we used as part of the validation. Our experimental framework and results are presented in Section V. Finally, we present our conclusions and future work in Section VI.

II. Power System Automation Elements and Threats

Modern power systems are designed to integrate an assortment of machinery designed to automatically monitor, control, and safeguard a system's operation, referred to as the "instrumentation and control (I&C) system". Substation automation is the process of collecting data from field devices with embedded computation and communication capabilities, i.e., intelligent electronic devices (IEDs), which are used to remotely control field devices. The IEDs are the robotic portion of the system implemented via highly specialized micro-processors called digital relays or, more commonly, programmable logic controllers (PLCs), which are programmed using hybrid automata. The intermediate instruments between a supervisory control unit (SCU) and field devices are the communication networks, including copper and fiber cables, wireless communication, and power line communication. In order to provide control and automation to power systems in an effective manner, various industrial control protocols have been adopted by the industry, including different versions of Modbus, DNP3, and IEC 61850, the latter which is specifically designed for substation automation systems.

The communication infrastructure of modern power systems provides attackers with the ability to remotely issue commands that can damage physical systems. When a fault occurs in the power transmission grid, protective digital relays isolate the faulted equipment by opening the adjacent circuit breakers. So, for example, an attacker even just performing a denial of service (DoS) attack can paralyze the system by preventing the exchange of valuable information, which can lead operators to make misinformed decisions.

In addition, knowledge of the transmission grid's configuration can be used to provide insight on how to create damaging

data injection attacks that bypass "bad data" detection algorithms. E.g., an attacker could fabricate meter measurements in a way that leads to false estimation of a power systems' state, such that the "bad data" monitors of current could not detect the attack [16]. Related to this, the ability of attackers to monitor network traffic, such as the data acquisition packet response sent by field devices to the control center, is also a vulnerability in the power transmission grid. Information such as the sender and receiver's addresses, and details of the transmitted messages can be obtained even if the packets are encrypted. Using this information, an attacker could perform traffic analysis attacks in order to obtain crucial information, such as bus voltage magnitude, and use this as a stepping stone for attacks that could actually damage specific parts of the grid.

III. Hybrid Control Network Intrusion System for Protective Digital Relays

Our *Hybrid Control NIDS (HC-NIDS)* provides a "hybrid" set of specification-based IDS rules by blending common network communication signatures with physical constraints that designate the physical system's expected operation. We first create the hybrid automaton that characterizes system's behavior, including both physical limits and communication patterns that the system should obey. From those, we derive the IDS rules and apply them to the network traffic exchanged within the cyber-physical system. To implement the IDS rules, we use the Bro Network Security Monitor, which includes IP packet parsers for two common industrial communication protocols, DNP3 and Modbus TCP. To demonstrate the efficacy of our approach, we developed several attack scenarios and implemented specification-based signatures that can identify those attacks as deviations from prescribed behavior. In the following, we describe a few of the IDS signatures and attack scenarios against which we evaluated the signatures.

A. Modeling the Behavior of Physical Systems

The hybrid model that characterizes the expected process of a physical system, such as the transmission grid, is a combination of three things: 1) a set of system equations that constrain analog quantities and depend on the state of the digital variables (hybrid state) or switches states, i.e, circuit breakers; 2) a controller program that routinely acquires sensor variables, compares them with physical conditions, and determines the pattern of information exchanged by PLCs to gather sensor data and issue physical or communication commands; 3) an application-layer protocol that codifies how message packets should be formatted and interpreted.

In this paper, we use a transformer's overcurrent protection scheme as an example of protection schemes implemented on the power transmission grid. The example consists of a three-phase, two-winding transformer that connects a generating unit to a transmission line. Two three-phase circuit breakers are connected to both sides of the transformer. We focus on the instantaneous overcurrent relay which provides rapid clearing of severe internal faults and external through-fault currents. The instantaneous overcurrent relay corresponds to device number 50 in the IEEE C37.2 standard [7], and is responsible for activating circuit breakers whenever the input current exceeds a predefined pickup current. The sufficient margin for the pickup current of the instantaneous overcurrent relay is between 125%-175% of the maximum low-side three-phase symmetrical fault current.

The expected behavior of the power transformer, based on our implementation, can be described as follows: for $N \in \{1, \cdots, 4\}$, let N denote the type of packet exchanged between the controllers, i.e., "read"/"write" command request/response, let I denote the measured value of the current that flows on the transmission line, and I_p denote a predefined pickup current. In the "no-fault" case, i.e., $I < I_p$, the circuit breakers next to the power transformer remain closed, i.e., $CB_1 = 0$ && $CB_2 = 0$. When a fault occurs, the circuit breakers are enabled, i.e., $CB_1 = 1$ && $CB_2 = 1$, in order to protect the system by preventing the flow of current on the transmission line. In both cases, the system remains at the same state until a new packet N is issued, where the type of the packet is directly related to the type of the previous exchanged packet. For example, a "read" request should be followed by a "read" response.

Each state is characterized by the operational status of the controllers (M/S), that indicates which controller is in active mode. The transition between the two cases is determined by the master controller $(M = 1, S = 0)$ after receiving a "read" response. In that stage, the master controller performs the overcurrent protection mechanism and if the measured current included in the "read" response exceeds the pickup current $(I \geq I_p)$ then the system switches to fault occurrence mode. When a cycle of commands is completed $(N = 4)$, the status of the automaton is reset, i.e., $N = 0$, and the execution is repeated based on the last observed situation.

In our implementation (as is typical of protection schemes) we do not observe the full state of the grid that dictates the line current. Therefore, the hybrid automaton describing our case study does not employ the differential and algebraic equations designating the flow of the continuous state (the value of current I vs. time). The hybrid automaton that corresponds to the system is shown in Fig. 1 and is the set H = (Q,X,f,Init,D,E,G,R), that consists of:

- $Q = \{q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7\}$ represents the set of discrete states;
- $X = \{I\} \in \mathbb{R}_{\geq 0}$ is the set of continuous states;
- $f(q_i, I) = g(\bar{V})$ specify the flow of the continuous state at a specific discrete state with $i \in \{0, \cdots, 7\}$;
- Init $= \{q_0\} \times \{I < I_p \wedge N < 1\}$ is the initial state;
- D specifies the assignment of the continuous state to each discrete state, e.g., $D(q_0) = \{I < I_p\}$;
- $E = \{(q_0, q_1), (q_1, q_2), (q_2, q_3), (q_3, q_0), (q_2, q_7), (q_4, q_5), (q_5, q_6), (q_6, q_7), (q_7, q_4), (q_6, q_3), (q_2, q_2), (q_6, q_6)\}$ is the set of edges;
- G is a guard condition, e.g., $G(q_0, q_1) = \{N = 1\}$;
- $R(q_3, q_0, N) = R(q_7, q_4, N) = \{N = 4\}$ are the reset mappings.

B. Hybrid Control Network Intrusion Rules

The HC-NIDS continuously monitors the network traffic of the physical system and executes the set of specification-based signatures that we implemented in order to identify events deviating from the expected operation of the physical system. Every Modbus TCP packet included in the network traffic is analyzed and characterized as acceptable or suspicious by

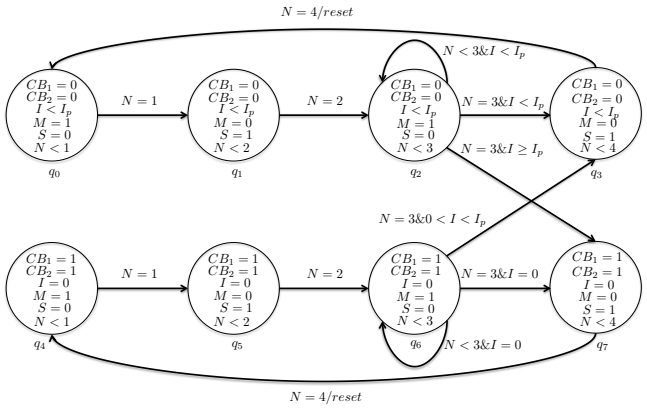

Fig. 1: Hybrid automaton for the case study

comparing specific fields of the packet to the HC-NIDS specifications. The HC-NIDS triggers an alarm in the form of a log entry whenever a deviation is observed. The small set of IDS signatures and scenarios that we describe in this section are derived from the expected behavior of a power transformer's overcurrent protection system. Our set of intrusion detection rules includes specifications that focus on the physical aspects of the system, based on the approach presented in this paper, in addition to specifications reflecting common security policies, e.g., check of acceptable IP addresses, and function codes (fc).

IDS Rule 1–Packet Sequence: The master controller continuously issues "read" requests to obtain the value of the current, and "write" requests to set the circuit breakers on a specific condition, reflecting the result of the overcurrent protection scheme. The expected packet sequence of the system is shown in Fig. 2. Due to non-deterministic packet ordering, a response does not always appear after the associated query. Therefore, we also use the transaction ID of the packets to check whether the appropriate pairs of packets are observed.

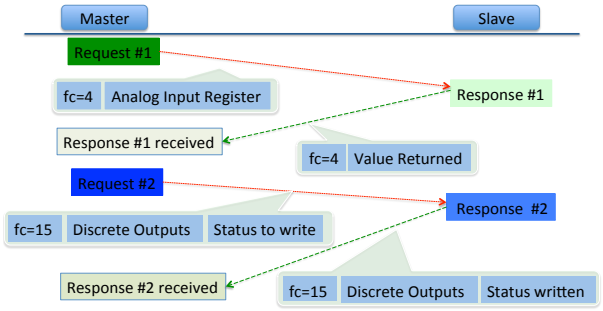

Fig. 2: Expected communication packet sequence

IDS Rule 2–Time Gap: The master controller issues queries with a specific rate, and the average time gap between a "read" and a "write" request in a cycle should fall within a specific range. Any deviation of this range indicates an attempt of possible illicit action, such as injecting packets that could activate the circuit breakers when it is not expected.

IDS Rule 3–Physical Constraints: The overcurrent protection scheme that we studied in this work is characterized by a pickup current that shows whether a fault occurred and the transformer should be isolated by activating the circuit breakers. In our implementation, we assume that the pickup current of the instantaneous overcurrent relay is 125% of the maximum low-side, three-phase, symmetrical fault current.

IV. Threat Model

In this section, we first define several levels of knowledge that might characterize an attacker's ability to circumvent our HC-NIDS and confuse or even damage the physical system. We then introduce several attack scenarios that we use to demonstrate and evaluate our HC-NIDS.

A. Attacker's Knowledge Level

In our attack scenarios, we consider various knowledge levels that might gauge an attacker's ability to penetrate into the system, based on the information that an attacker could obtain in order to confuse the electrical physical system.

1) *Zero or Low:* Limited knowledge about the network communication rules, such as IP addresses of the controllers and the communication protocol used within the system.
2) *Moderate:* The attacker fingerprints the master and slave controllers, identifying information about IP addresses, and memory mappings to physical devices.
3) *Privileged:* The attacker obtains knowledge about the IP addresses used by the controllers, the command function codes used, and communication patterns of packets that involve manipulating the physical behavior of the system.
4) *Sophisticated:* The attacker gains complete access to the network traffic, and also has access to sophisticated tools that assist in analyzing the network traffic and extracting integrated information about the physical process.

B. Attack Scenarios

In order to evaluate the performance of our HC-NIDS in protecting the power transformer's physical model, we examine several attack scenarios aimed at perturbing the normal operation of the system. Our evaluation focuses on attack scenarios that our HC-NIDS is able to identify through specification-based intrusion detection rules related to physical operation of the system. Our rules are built using the Bro IDS, and as with any general-purpose NIDS, Bro is capable of detecting attacks relevant to typical communication policies, including the IP addresses of the controllers. Therefore, to demonstrate that our approach of protecting physical systems functions perfectly well alongside rules that focus only the traditional network protocol aspect, our scenarios include examples of both "cyber" and "physical" attacks.

1) Injecting Malicious Packets: The goal of this attack is to isolate and disable the power transformer by activating the circuit breakers. The attacker obtains a "moderate" level of awareness, which does not include information about average time gap or expected packet sequence of commands. Our HC-NIDS detects this type of attack by checking the consistency of the expected packet sequence via IDS Rule 1.

2) Isolating the Power Transformer: This attack is similar to the first attack scenario, which aims to cut off the power transformer from the rest of the transmission line. We assume that the attacker is capable of acquiring details related to communication patterns of packets that are included in the anticipated behavior of the system, and correspond to the "privileged" level of knowledge. However, we assume that the

attacker is not aware of the average time gap between a "read" and a "write" command request. Our HC-NIDS detects this type of attack via IDS Rule 2.

3) Imitating the Master Controller's Behavior: This attack scenario is similar to the attack that tries to isolate the power transformer when it is not required by the overcurrent protection scheme. The attacker obtains a "privileged" level of awareness, which includes information about the expected packet sequence of commands. However, we assume, as it is inferred by the definition of the knowledge level, that the attacker is not aware of the overall system's expected operation, and does not know about the physical constraints applied to the overcurrent protection scheme. This type of attack is directly related to our "hybrid" set of intrusion detection rules, and is identified through IDS Rule 3.

V. Experimental Analysis

In this section, we first introduce the experimental framework that we developed to simulate the operation of a power transformer and validate our approach. We then present the results of applying the specification-based IDS rules associated with the normal physical operation of the simulated case.

A. Experimental Framework

The experimental framework that we developed allows us to establish communication between a simulated physical process and a real PLC through an Ethernet interface that sends information via the Modbus TCP protocol. While many transmission systems rely on more advanced options, the choice of Modbus for our experiment is dictated by practical convenience (inexpensive PLC a variety of software tools and a library). However, the ideas discussed are applicable to many of the application layer protocols used in I&C. The developed testbed is shown in Fig. 3, and includes the following levels:

1) Simulink model of the physical application
2) C MEX S-function that allows communication through the Modbus TCP protocol
3) Emulation of the control mechanism in ladder logic.

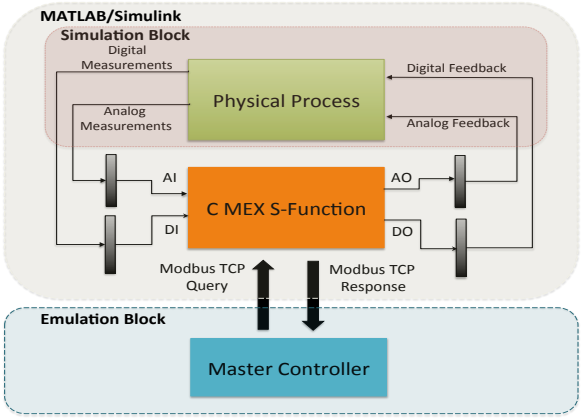

Fig. 3: Block diagram of the experimental framework

In the first level, we implemented the operation of a power transformer in the Simulink simulation environment. In our work, we assume that the transmission line, including a three-phase transformer, circuit breakers, measurement sensors, etc., corresponds to the physical process that we want to protect using the overcurrent protection function. Moreover, in our simulation block, we consider current sensors that continuously record measurement samples of the current that flows on the transmission line, and feed the block that is responsible for the Modbus packet transmission (S-function block) and which constitutes the slave controller.

In the second level, we developed an S-function block that we implemented in ANSI C, that formulates Modbus responses based on the master controller's queries. The current sensors included in the dynamic model provide the S-function block with the appropriate physical measurements, which are used in the next level in order to check the consistency of the physical model. The S-function block formulates packets that include the input measurements, and dispatches the Modbus packets to the master controller whenever a "read" query is received. The S-function block also performs the feedback control actions specified in the "write" query, which the master controller sends after the overcurrent protection functions are executed.

The third level of our testbed includes a Siemens SIMATIC S7-1200 PLC that acts as the master controller and performs the overcurrent protection function related to the physical system. The master controller initiates a connection with the simulated slave relay and polls the slave in order to acquire the value of the input measurements obtained by the current sensors. Then, the protection control algorithm is executed and, based on the result, the master controller sends "write" queries to the slave relay that indicate which control action should be performed, i.e., activate a circuit breaker in the case of fault.

B. Evaluation of Attack Scenarios

Our experimental results demonstrate the capabilities of our HC-NIDS for detecting a wide range of attacks by using the physical constraints and the overall expected behavior of the studied physical system in addition to the common communication rules that are included in our HC-NIDS.

1) Attack Scenario 1: The packet sequence of the issued commands that appear in the network traffic do not conform to the expected packet sequence that our IDS rules in the HC-NIDS specify. Fig. 4 shows an instance of the network traffic of the exchanged communication packets between the slave controller and the polling devices in the form of Modbus TCP/IP queries and responses.

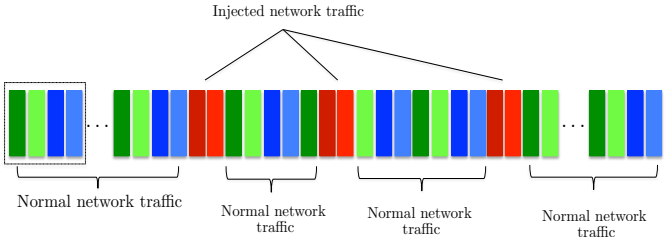

Fig. 4: Sequence of packets in the network traffic

We expect to observe a repetitive pattern of packets in the network traffic, which consists of two pairs of packets, i.e. "read" commands (green bars) and "write" commands (blue bars). In Fig. 4, red bars indicate the identified illicit actions, in the form of injected packets, in between the packets that correspond to normal network traffic. Our HC-NIDS identifies the attempt to activate the circuit breakers next to the power transformer, and issues alerts indicating an unacceptable packet sequence of issued commands.

2) Attack Scenario 2: The attacker issues packets that conform to the general communication rules, included the utilized command function codes, and the expected packet sequence. Initially, a "read" command request is dispatched in order to acquire a knowledge of the value of the current. Then, the attacker sends spurious "write" requests to activate the CBs to isolate the power transformer from the transmission line. Our HC-NIDS computes the time gap between the two packets, observes that the time difference does not comply with the preconcerted average time gap, and generates an alarm indicating the illicit action.

3) Attack Scenario 3: The attacker sends "write" requests either to activate the circuit breakers (status = 0), and isolate the power transformer when it is not necessary, or to prevent the circuit breakers from activating (status = 1) when the power transformer's current exceeds the predefined pick-up current. Fig. 5 shows the measured current of the power transformer, and subsequent actions regarding circuit breakers' status. Even though each packet is a legal event on its own, the *combination* of the packets constitutes an illicit event since the physical constraints specified by the normal operation of the system are not met. Our HC-NIDS identifies the attacker's activity by checking the consistency between the measured current of the power transformer and the status of the circuit breakers, and generates alerts indicating the damaging activity.

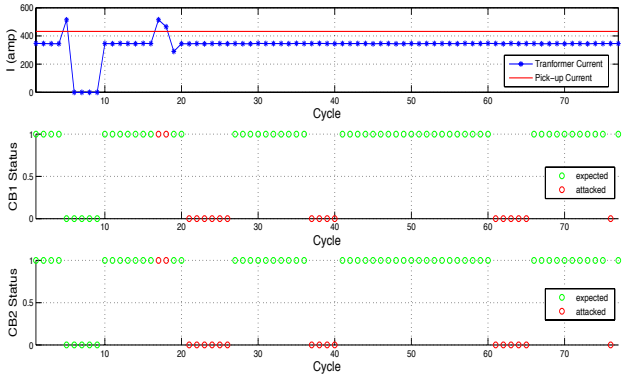

Fig. 5: Transformer's current and status of circuit breakers

VI. Conclusions and Future Work

The power transmission grid plays a vital role in society by assuring reliable transfer of electrical energy from power plants to customers. In our work, we highlight the importance of combining both network and physical information in the form of specification-based intrusion detection rules to ensure the reliable and secure operation of components of the power grid. Although in this paper we focus on certain aspects of the transmission grid, we believe that it could be extended to other systems that present a similar operational behavior.

A number of open challenges remain. For example, we have shown our approach can be effective for small parts of a cyber-physical system, but such systems often consist of many components requiring coordination in order to ensure safe operation of the entire system. Using many IDSs that collectively monitor numerous control aspects presents a coordination and timing challenge. Also, in our attack scenarios, we assume that an attacker does not have complete knowledge about the physics of the system. For more attackers with more detailed information, rules with more detailed physical knowledge would be required by our HC-NIDS to enable it to detect more sophisticated attacks. Finally we note that the hybrid automaton and IDS rules must be customized for each application with different physical limits and settings. Producing a more generalized approach to developing rules from physical specifications is a subject of future research.

Acknowledgements

This research was supported in part by the Director, Office of Computational and Technology Research, Division of Mathematical, Information, and Computational Sciences of the U.S. Department of Energy, under contract DE-AC02-05CH11231. It is also supported in part by the Department of Energy under Award Number DE-OE0000097 and by the National Science Foundation under Grant Number CCF-1018871. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect those of the sponsors of this work.

References

[1] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and Evaluation of Security Threats on the Communication Networks in the Smart Grid," in *Proc. Military Communications Conference (MILCOM)*. IEEE, 2010.

[2] Y. Deng, S. Shukla *et al.*, "Vulnerabilities and Countermeasures–A Survey on the Cyber Security Issues in the Transmission Subsystem of a Smart Grid," *J. Cyber Security and Mobility*, vol. 1, no. 2, 2012.

[3] B. A. Carreras, D. E. Newman, and I. Dobson, "Determining the Vulnerabilities of the Power Transmission System," in *Proc. 45th Hawaii International Conference on System Sciences (HICSS)*, 2012.

[4] E. Zio, C.-A. Petrescu, and G. Sansavini, "Vulnerability Analysis of a Power Transmission System," in *Proc. International Probabilistic Safety Assessment and Management Conference (PSAM)*, 2008, pp. 18–23.

[5] B. Mukherjee, L. T. Heberlein, and K. N. Levitt, "Network Intrusion Detection," *IEEE Network*, vol. 8, no. 3, pp. 26–41, 1994.

[6] T. A. Henzinger, *The Theory of Hybrid Automata*. Springer, 2000.

[7] "IEEE Standard Electrical Power System Device Function Numbers, Acronyms, and Contact Designations," *IEEE Std C37.2-2008*, Oct 2008.

[8] R. Mitchell and I.-R. Chen, "A Survey of Intrusion Detection Techniques for Cyber Physical Systems," *ACM Computing Surveys*, vol. 46, no. 4, 2013.

[9] T. H. Morris, B. A. Jones, R. B. Vaughn, and Y. S. Dandass, "Deterministic intrusion detection rules for MODBUS protocols," in *Proc. 46th Hawaii International Conference on System Sciences (HICSS)*, 2013.

[10] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," *Procedings of the IEEE Symposium on Security and Privacy*, 2010.

[11] A. Carcano, I. N. Fovino, M. Masera, and A. Trombetta, "State-Based Network Intrusion Detection Systems for SCADA Protocols: A Proof of Concept," in *Critical Information Infrastructures Security*, ser. LNCS. Springer, 2010, vol. 6027.

[12] R. Berthier and W. H. Sanders, "Specification-Based Intrusion Detection for Advanced Metering Infrastructures," in *Proc. 17th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC)*, 2011.

[13] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks Against Process Control Systems: Risk Assessment, Detection, and Response," in *Proc. ACM Symposium on Computer and Communications Security*, 2011, pp. 355–366.

[14] M. Parvania, G. Koutsandria, V. Muthukumar, S. Peisert, C. McParland, and A. Scaglione, "Hybrid Control Network Intrusion Detection Systems for Automated Power Distribution Systems," in *Proc. 1st Intl. Workshop on Trustworthiness of Smart Grids (ToSG)*, 2014.

[15] V. Paxson, "Bro: a System for Detecting Network Intruders in Real-Time," *Computer Networks*, vol. 31, no. 23, pp. 2435–2463, 1999.

[16] L. Xie, Y. Mo, and B. Sinopoli, "False Data Injection Attacks in Electricity Markets," in *Proc. IEEE SmartGridComm*, 2010.