A Specification-based Intrusion Detection Framework for Cyber-physical Environment in Electric Power System

Shengyi Pan, Thomas Morris, and Uttam Adhikari
(Corresponding author: Shengyi Pan)

Department of Electrical and Computer Engineering, Mississippi State University
Box 9571, 216 Simrall Hall Mississippi State, MS 39762, USA
(Email: tommymorris@ieee.org)

(Received June 13, 2013; revised and accepted Nov. 2, 2014)

Abstract

The emergence of high-speed networks in electric power systems creates a tight interaction of cyber infrastructure with the physical infrastructure and makes the power system susceptible to cyber penetration and attacks. To address this problem, this paper proposes an innovative approach to develop a specification-based intrusion detection framework that leverages available information provided by components in a contemporary power system. A Bayesian network is used to graphically encode the causal relations among the available information to create patterns with temporal state transitions, which are used as rules in the proposed intrusion detection framework. This allows the proposed framework to detect cyber attacks and classify different substation scenarios. A case study is provided for the non-pilot directional over current relay protection scheme for a modified 2-bus 2-generator system taken from a section of the IEEE 9-bus 3-generator system. Nine power system scenarios were developed and implemented as part of the case study. Each scenario was implemented on a test bed and all scenarios were correctly classified by the IDS built using the proposed methodology.

Keywords: Bayesian network, cyber-physical, electric power system, intrusion detection system, relay protection scheme, synchrophasor

1 Introduction

The next generation electric power grid will rely on many advanced technologies such as synchrophasor systems, industrial automation control systems and advance metering infrastructure in order to meet the increasing demand on reliable energy. Due to the critical role that the electric power system plays in our society, there is a common agreement among different organizations that the electric power grid needs to be better secured to ensure continually available power being provided to the nation [35]. The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) program defines critical infrastructure and provides recommendations regarding to cyber security for electric utilities to better protect their critical infrastructures [38]. The National Institute of Standards and Technology Interagency Report (NISTIR) 7628 also documents the guidelines and requirements for industry to better secure their facilities [15]. However, the United States Government Accountability Office (GAO) has realized that current guidelines from these organizations are not sufficient to securely implement the modern electricity grid and it calls for the retrofit research and development to current security mechanisms [12].

1.1 Background and Problem Statements

The cyber-physical security issues of electric power systems have been discussed for a long time. In the past the electric power system was often isolated and used proprietary devices and software. The contemporary and future power grid uses advanced technologies which rely on the commercial off-the-shelf (COTS) components e.g. Personal Computers (PCs), Windows Operating System, and standardized communications such as IEC 61850 and IEEE C37.118. Many COTS components were designed for consumer or enterprise use and not for use in critical infrastructures such as the electric power system [10]. Power system cyber components have certain security features (password authentication) built in, however, penetration tests conducted in [30, 33] have shown that cyber attacks targeted towards substation computers and devices can interrupt the electric power system communications, prevent real time monitoring of the power system, induce physical side effects. Hence there is a need to develop security countermeasures that can be deployed to protect the critical infrastructures in the electric power system. However, a barrier for developing cyber security countermeasures is a lack of algorithms based on the unique characteristics of electric power system where high interactions between the physical process and the cyber infrastructures are present [44]. The cyber infrastructures provide the communication media that is used between the physical automation control system and other systems such as enterprise software where control algorithms or system analysis algorithms are implemented. Since most of the cyber infrastructures use open standards without security features, once they are compromised, the attackers are able to launch attacks targeting the physical process by modifying the control algorithm. An example is the resonance attacks where an attacker who compromised the sensors or controllers causes the physical system to oscillate at its resonant frequency [7]. Another example is demonstrated in [27] where an attack can inject false data to compromise meters to bypass the existing bad data detection algorithms. An example of attacks from physical devices in real world is the Stuxnet in July 2010 where the malware targeting control system physical devices spread by USB drives [11]. Some recent works investigating the security issues in the modern electric power grid suggest that new security mechanisms should focus on the unique characteristics of the power grid to achieve comprehensive protection [32, 47].

Since attacks are always unpredictable and cannot be eliminated, it is necessary to deploy an intrusion detection system to alert operators or automated response algorithms when an attack is discovered. Traditional intrusion detection systems that only examine network traffic cannot provide enough detection abilities to the cyber-physical system where the physical process is also of concern [7]. In this paper, a new methodology that extends the ability of traditional anomaly-based intrusion detection system is proposed to design an intrusion detection system suitable for cyber-physical system by taking the system's physical process into account. The proposed intrusion detection system is able to provide a "defense-in-depth" protection by considering the following two concerns [6]: The consequences of the attacks on the cyber-physical system should be understood when planning the protection; and novel attack-detection algorithms should be developed based on how the physical process should behave so that intrusion detection systems can identify whether the control command or sensor data has been altered.

In addition, another concern from utility operators is that cyber security solutions should make minimum modification to the current facilities in the grid. This is because any changes to be made require strict recertification and evaluation to be adapted to the grid, which can be quite costly [17]. Therefore, the security solution proposed here is designed to be built upon current resources in the grid minimizing changes to its components.

1.2 Contributions of This Paper

This paper addresses the security challenges of the modern cyber-physical electric power system by proposing an intrusion detection framework that covers the aforementioned three concerns. This framework provides a specification-based intrusion detection system that complements current anomaly intrusion detection systems by leveraging time-synchronized data from synchrophasor devices as well as observable events from audit logs of network devices including protection relays, network monitoring software, and control room computers. Depending on different control schemes, this information underlines causal relations between the system behaviors in the cyber-physical system. One of the contributions of this work is to provide a methodology to map such information to the probabilistic network - Bayesian network to derive the rules for the IDS. The Bayesian network is recognized for its powerful intuitive method of modeling interdependencies between variables and its ability to graphically represent causal relations from data and workflow logs. Based on a specific control scheme, namely the over current relay protection scheme, this paper demonstrates the procedure to construct such a Bayesian network and derive the temporal-state transition patterns for different system scenarios. These patterns are used in the IDS as rules for classifying legible system scenarios and detecting intrusions that aim to interrupt the protection scheme. A model to implement the proposed IDS is also provided based on a specific power system transmission system test bed. The IDS monitors the status of one relay and the transmission line where the relay is located to provide an extension to power system situation awareness such that the operator can be informed of whether disturbances in the power grid (e.g. faults in transmission line or relay operations) are caused by system faults or cyber attacks.

1.3 Paper Organization

The rest of the paper is organized as follows. First, related works are discussed in Section 2. Section 3 provides an overview of a reference electric transmission system, the non-pilot over current protection scheme, and a hardware-in-the-loop test bed implementation of the transmission system and protection scheme. This system is used later in the paper for case study to demonstrate the effectiveness of the proposed IDS methodology. Section 3 also provides a threat model which describes 9 power system disturbances and cyber attacks which threaten the reference transmission system and protection scheme. Section 4 provides a mathematical description of the Bayesian network and discusses a procedure for creating a Bayesian network for a cyber physical system. Section 5 provides results an analysis of the IDS built for the case study. Conclusions and future work are discussed in Section VII.

2 Related Works

2.1 Wide Area Monitoring Systems

The need of electric market regulation and the connection of neighboring grids motivate the Wide Area Monitoring System (WAMS) where multiple organizations cooperate to allow real-time monitoring of the electric power system. The WAMS is a measurement system that uses information communication technology (ICT) to transmit digital and/or analogue information. The WAMS is now adopting time-synchronized data that provides microsecond time accuracy [29]. The time-stamping data in WAMS includes not only the measurements such as phasors of voltage, current (i.e. synchrophasor system) but also the status of some IEDs such as relays, breakers etc. [2]. Such accurate redundant information nowadays can be collected from PMUs, smart meters and protection relays etc. The redundant information contributed by the time-synchronized data provides benefit for reliability, efficiency, and economics in power system monitoring and control. The extreme low latency brought by time-synchronized data allows various real-time wide area control algorithms and special protection schemes to be developed to increase power grid reliability and stability [2, 18, 21, 28, 34]. This paper takes advantage of this fast and accurate information provided by synchrophasor system to build a novel intrusion detection system for the electric power system.

2.2 Specification-based Intrusion Detection System

The idea of intrusion detection systems was originally introduced to the IT system to detecting activities that violate security policy [37]. There are two types of intrusion detection systems (IDS): Misuse-based Intrusion Detection Systems and Anomaly-based Intrusion Detection Systems. Misuse-based IDS and signature-based IDS look for well-defined patterns of known attacks or vulnerabilities, and, therefore, suffer from the fact that any undefined attacks will be ignored [49]. Anomaly-based IDS consider the normal behaviors of a system [13, 54]. Any derivation from the normal system behaviors will be defined as an intrusion. The anomaly-based IDS is widely used for its ability to detect zero-day intrusions however, it has high false positive rate where some normal behaviors of the system that do not match the defined normal behaviors will be mistaken as intrusions. The specification-based IDS was introduced by Ko in 1996 [24] as a complement to the anomaly-based IDS to improve its accuracy. Specification-based IDS monitor the system according to policies specified by valid sequences of system behaviors. Any sequence of behaviors outside the predefined specifications will be regarded as a violation. Various methodologies have been applied by scientists to specify such behavior/event sequences, for example, the parallel environment grammar [24], regular expressions for events [50], or abstract state machine language [43]. The specification-based intrusion detection has also been widely applied in software engineering. Most recently specification-based intrusion detection is also used in the area of network protocol of critical infrastructures e.g. ANSI C12 protocol for advanced metering infrastructure [3], DNP3 protocol [26], IEEE C37.118 protocol [46], Modbus protocol [9]. The specification-based IDS is popular in this area because network protocols usually have standard message formats from which the specifications of the IDS can be derived. The applications of specification-based IDS also extend to more complex systems such as networked SCADA systems [5], medical cyber-physical systems [31] and real-time embedded systems [55] where intrusion detection rules are defined from system behaviors. The system behaviors in these works are represented by a sequence of system states. By keeping tracking the system state the intrusion detection techniques of these works discover the malicious activities that drive the system state from safe to unsafe. This paper puts emphasis on cyber-physical electric power grid. In addition to define a finite state machine for the electric power system, this paper uses a probabilistic network to extract knowledge about the specifications of different system behaviors from the causal relationship underlined by the transitions of these system states. Such knowledge is used to derive the rules used by the proposed IDS to classify system behaviors.

2.3 Why Bayesian Network?

Probabilistic networks provide clear semantics to allow them to be processed for extracting knowledge of a certain domain. They are able to represent the dependencies or interdependencies between variables; therefore they can be used for diagnosis, learning, explanation, and many other inference related tasks necessary for intelligent systems [4]. Among the probabilistic networks, the Bayesian network is prevalent for its explicit graphical representation of cause-effect reasoning with uncertainty. Depending on different interpretations, it can also represent causality. One of the applications of Bayesian networks is in network vulnerability assessment where "attack graph" is developed using a Bayesian network [52]. In an attack graph, two directly connected nodes represent the causal relation in which the compromise of one node will lead to the compromise of the other node. In addition, Bayesian networks have also been applied to interdependency modeling and analysis for critical infrastructure [14, 16] and for fault diagnosis in power systems [36, 53]. In the area of health care, Bayesian networks are also used to discover patterns for Hemodialysis to help medical professionals react to exceptions [25]. Tutorials about Bayesian networks can be found in [8, 23, 40]. In the cyber-physical environment, a sequence of system actions and events raised by a specific system scenario (e.g. a short circuit fault in a transmission line) imply the causal relations between system states. The causal relations are represented as tempo-

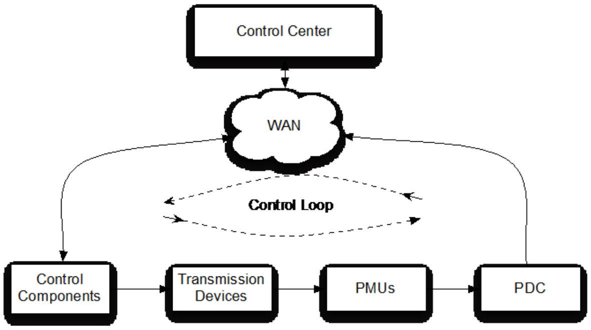

Figure 1: Structure of electric transmission system with integration of synchrophasor Technology

ral transitions between different system states. Therefore, the system states are nodes in the Bayesian network.

3 System Model and Threads

In this section, a brief introduction of the electric transmission system integrated with synchrophasor technology will be given. The potential attacks and their consequences to the transmission line protection scheme will be discussed on the basis of a 2-generator 3-bus electric transmission system. Nevertheless, all discussions are based on the assumption that the attacks are launched after the attackers compromise the substation communication network or physically penetrate the substation such as through an insider attack by a disgruntled employee authorized to access power grid facilities and or its communication network.

3.1 Cyber-Physical Environment of Synchrophasor-based Electric Transmission System

A typical power system is divided into four functional parts: generation, transmission, distribution and consumers. The electric transmission system is the backbone of the power system transmitting the electric power from generators to the load centers over a long distance. The structure of a cyber-physical environment for the electric transmission system augmented with synchrophasor technology is shown in Figure 1. The transmission system devices are mainly composed of transmission lines, breakers, and transformers that are monitored by field sensors. In the case of a synchrophasor system these field sensors are Phasor Measurement Units (PMUs). The PMUs attached to transmission lines provide synchronized data that is time-stamped to the Coordinated Universal Time (UTC) via Global Positioning System (GPS) signals for continuous real-time monitoring. Phasor Data Concentrators (PDCs) collect synchrophasor measurements from PMUs that are located in different locations and send the measurements to the control center through the wide-area network (WAN). PMUs in different locations and PDCs are key components in the synchrophasor based wide area monitoring system (WAMS). Compared to the traditional supervisory control and data acquisition (SCADA) system where the field sensors measure the system once per several seconds, the emergence of WAMS leveraging synchrophasor technology allows much faster measuring for the transmission system at the rates ranging from 30 samples per second to 120 samples per second. The control center that utilizes the high resolution measurement data aggregated by PDCs is able to evaluate the system status and perform advanced algorithms to make different real-time control decisions to control components in the field. The information flow described above is shown as the dotted line in Figure 1 and is often recognized as a control loop. All devices in this system are synchronized to UTC time via GPS signals. However, in the case of a distributed control, the protection components in the system sense the disturbance and react to it by themselves. The bi-directed-arrow lines in between control components and WAN indicates not only the command data sent from control center but also the time-synchronized audit information reported from intelligent electronic devices (IDEs) to the control center.

The system can be considered as a finite state machine. If, for example, a tripping operation is sent from control center, this will cause system state transitions because a signal-sending operation has been recorded in the control panel which is one component of the system. In general, the changes of the behaviors in different system components such as a breaker, relay, and transmission lines in a given period of time or at a definite point of time will cause the system state to transit from certain state to another. Theses changes are reflected by the transmission line sensor readings or device logs. If the system state is represented as a set of observations (from logs of different components) and measurement data (from measurement devices) inside the system, such changes along with time can be regarded as temporal state transitions.

3.2 Reference Electric Transmission System and Non-pilot Over current Protection

Non-pilot transmission system protection is chosen as a demonstration vehicle for the proposed IDS because this type of protection is fundamental to all other electrical equipment [19]. The non-pilot directional over current relay protection scheme is examined in the context of a multiple source circuit shown in Figure 2 to provide protection against short circuit faults which are the primary disturbances found in transmission lines. This paper focuses on multiple source circuits. Although there may be other types of circuits such as loop circuit and radial circuit, multiple source circuits make up the majority of the electric transmission system. The IDS proposed here is suitable only to the multiple sources circuits where our assumption that when one line is taken off the load can still get supplied from generators via other route can be

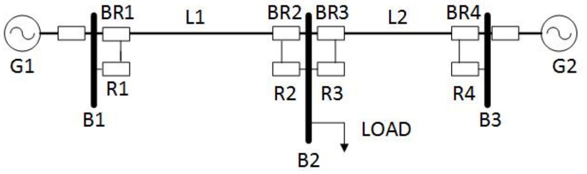

Figure 2: Single line diagram for over current protection scheme for a transmission system

true.

In a multiple sources transmission system, the relays are directional to provide relay coordination between all of the relays that can see a given fault. In this paper, instantaneous and time-delay over current relays are applied to the transmission system to provide a directional over current protection scheme for a maximum of 2 zones. Readers can refer to [19] for a complete introduction of non-pilot over current protection of transmission lines.

The single-line electric transmission diagram depicted in Figure 2 is a modified 2-bus 2-generator system taken from a section of the IEEE 9-bus 3-generator system [45]. In the non-pilot system, relays decisions solely depend on the measurement of electrical quantities at the near end of the protected line section. Generators G1 and G2 supply power to load L at bus B2 via the transmission line L1 and L2. Line L1 and L2 are symmetric. The load can be changed from 200 MW to 240 MW in this study. Four relays R1, R2, R3 and R4 with integrated PMU functionality reside at each end of each transmission line that control the breakers BR1, BR2, BR3 and BR4. Take line L1 for example, the relays R1 and R2 provide instantaneous over current protection for transmission line L1 while R1 also provides time-delayed over current protection for transmission line L2 in the case that the relay R3 fails for faults in L2. It is the similar case to the relays in line L2 where R3 and R4 take care of the faults in L2 and R4 provides backup protection for faults in L1 in case R2 failed tripping for the fault. For the four relays, there are two settings that should be properly configured to achieve the over current protection and relay coordination: the instantaneous over current pickup and the time-delayed over current pickup (abbreviated as IOC and TOC). The IOC specifies the threshold so that the relay will operate for all short circuits which cause the current magnitude to exceed the threshold in the line it is to provide protection for. As for the two-zone over current protection a TOC specifies the threshold according to which the relay provides backup protection for an adjacent line. In this case, the relay wait for a period of time called ”delay time” if the current magnitude is in the ”warning level” (magnitude in between TOC and IOC) in the local line, which indicates a short circuit fault in the adjacent line. Theoretically relay trips simultaneously when PMU displays overcurrent for instantaneous over current protection, but the simulation in this paper will insert one cycle delay between them, which is more likely in the real situation.

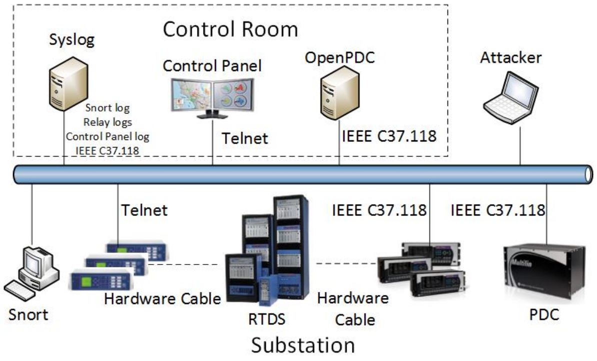

Figure 3: Test bed topology

The four PMUs constantly monitor the power flow in the two transmission lines at the locations where the relays sit. They transmit time-stamped synchrophasor data in the IEEE C37.118 data frames [48] to a PDC in the substation via Ethernet in a frequency at 120 samples/second. The data frames including information of angles and magnitudes of line current and voltage, namely phasors, will be finally stored in a historian located in the control room. Usually, an Energy Management System (EMS) with an integrated software PDC (e.g. OpenPDC [20]) is installed in the control room for applications such as system visualizations, system situation awareness etc. [56]. The software PDC is a higher level PDC that collects synchrophasor data frames from physical PDC devices in different locations and processes them. The operator who monitors the system status through a software PDC will be kept informed to react to a contingency in the monitored system.

3.3 Test Bed Configurations

A test bed was implemented to simulate the electric transmission system shown in Figure 2. The test bed includes the real-time power system simulator (RTDS) with a hardware-in-the-loop design using commercial PMUs, PDCs and protective relays [1]. The topology of test bed is depicted in Figure 3.

The test bed is separated by the Ethernet bar into two parts. In the substation site, the RTDS is used to model the 2-bus 2-generator transmission system discussed shown in Figure 2. There are four commercial digital relays with integrated PMU functionality connected to breakers simulated in the RTDS. The RTDS provides simulated high AC voltages at buses and line currents through transmission lines for the PMU and relays to measure. The relays and PMUs are drawn as two separate components in Figure 3. In some cases the PMU and relay are integrated in the same chassis. In other cases the PMU and relay are separate devices. The RTDS simulates single line to ground and the phase to ground short circuit faults on transmission lines L1 and L2. The hardware-in-the-loop design allows the relays to react to the fault to open the breaker. The four PMUs reside at the two ends of line L1 and line L2 constantly measure current and voltage phasors. There is one hardware PDC in the substation that aggregates IEEE C37.118 synchrophasor measurements from the four PMUs through the substation network switch and forwards the concentrated synchrophasor measurement data frames to the control room where OpenPDC is installed. OpenPDC displays and stores the synchrophasor data and serves as a data historian for the system. The substation is also equipped with Snort to monitor the substation network traffic. In our experiment Snort [51] is configured to capture Telnet frames that contains tripping commands to the relay. The content of the tripping commands varies by the relay brand and model. However, whenever the Snort rule captures remote tripping commands, it logs them with their source IP address and destination IP address (relay IP address). The content in the Snort log file is forwarded to a syslog server in the control room. In the control room, the control panel is a Microsoft Windows PC with vendor-provided configuration clients for the relays and PMUs. Relay and PMU configuration can be performed either remotely over the communications network or from the devices' faceplate.

Relays in the test bed are specifically configured to implement the directional over current protection scheme for the 2-bus 2-generator transmission system. Two relevant parameters in the relay configurations are of concern to the IDS: IOC, TOC. The PMUs and PDC are configured to stream in the data rate of 120 samples per second. Each relay is operated independently according to configurations and opens its corresponding breaker in the transmission lines. Breaker failure is also simulated in this work, in which the relay trips but the corresponding break does not open. There are four situations that relay will be tripped: (1) Relay detects fault occurring in the direction it faces; (2) Attackers send tripping command to relay via Telnet from their PCs; (3) Attackers trip the relay via its faceplate; (4) The operator sends tripping command to relay via Telnet from control panel. The test bed also provides time-synchronized audit data from logs of multiple components. In addition to Snort log which is used to record time stamped remote trip command, PMU measurements are used as a redundant source of line current measurements. Relay logs are used to record time stamped relay operations. The control panel log records time stamped commands to the energy management system to trip a relay. This information is aggregated in the syslog server and used to track series of causal events related to different system scenarios.

3.4 Scenarios for Over Current Protection Scheme in Line L1

This threat model consists of a set of scenarios which represent normal power system disturbances, normal supervisory control actions, and cyber attacks against the nonpilot directional over current protection scheme. Each scenario has been implemented using the test bed described in the previous section. A comprehensive understanding of these scenarios is important for the domain expert to identify which information is required from which resources to construct the IDS.

For this work it is assumed attackers attack only one relay or PMU at a time. There are two legitimate scenarios for over current protection scheme for line L1. Scenario Q1 is an over current fault on line 1 which causes R1 and R2 to instantaneously trip. Scenario Q2 is the removal of a line L1 for maintenance. In scenario Q2 an operator initiates a remote trip of R1 and R2 via the energy management system. The operator initiated remote trip commands will be recorded in the control panel log with the timestamps showing when the commands were sent. The remote trip events are also logged by the network traffic monitor, Snort. The trip commands cause the relays to open the breakers isolating line L1 from the power system. The operator observes the success of breaker-opening action by observing zero current in L1 from synchrophasor data frames collected by OpenPDC.

The attacks considered for this work focus on changing the control logic. To achieve this goal, attacks attempt to interrupt the over current protection scheme on line L1 by causing relays to not trip during a valid fault or by causing relays to trip when there is no fault. The operator in the control center may be aware of the implications of the aforementioned attacks via the collected synchrophasor data however he/she will still lack information on the primary cause of these failures. In this paper, we will analyze such failures from security perspective.

Scenario Q3 is a cyber command injection attack which mimics scenario Q2. For scenario Q3 the remote trip command does not originate from the control panel. Instead the remote trip command originates from another node (i.e. attacker's PC) on the communications network. As such, the control panel log will not include a trip command entry, but, the network traffic monitor will detect the remote trip command. Scenario Q4 is a physical attack in which an attacker trips the relay from the faceplate. In Scenario Q5 a valid fault occurs, but, the relay does not trip. This may occur due to hard ware error or incorrect relay setting. Scenarios Q6, Q7, and Q8 are data injection attacks which provide false current measurements to the operator by modifying synchrophasor measurements. In scenario Q6 current magnitudes above the relay pickup are injected to the PDC and transmitted to the control room. This scenario attempts to cause the operator to believe a set of relays has failed to operate and therefore cause the operator to manually trip the relay. In scenario Q7 the injected current magnitudes are less than the relay pickup. This scenario may be used to mask a fault which has been handled by relay which has been tampered with. In scenario Q8 the injected current magnitudes are 0 amperes. This scenario attempts to mimic the situation immediately after a properly handled fault. Scenario Q9 is for scenarios which target other relays. A separate instance of the IDS monitors each relay. Scenario

Q9 simulates breaker failure where the relay tripped but the current in the line remains high due to the breaker failure. According to the assumption that only one malicious activity takes place at a time, the breaker failure is simulated only when there is a fault in the line. Scenario Q10 is for scenarios which target other relays. A separate instance of the IDS monitors each relay. Scenarios Q1-Q9 are used to classify local events and scenario Q10 classifies events at other relays.

4 Constructing Bayesian Network for System Scenarios

In this section a set of terms are introduced. These terms are defined to mathematically describe Bayesian networks used to model the 10 scenarios from the threat model. Next the procedure to construct the Bayesian network with temporal state transitions for relay R1 is demonstrated. Patterns for the 10 scenarios are derived from the Bayesian network. These patterns are then used as detection rules for the IDS which monitors R2.

4.1 Definitions

A state represents system status at a point in time. A state is defined as a set of variable, each of which is a measurement. A state is denoted as $S = \{v_1, \cdots, v_n\}$. Each state variable in state S i.e. $v_1 \in S$ may have a unique range called its own domain donated as D_j. The number of possible distinct values, $\|D_j\|$, varies by components. Domains should be quantized to finite ranges to avoid infinite state space. D_j is hence denoted as a set of distinct values $\{d_j1, \cdots, d_{j\|D_j\|}\}$ with each of its elements specifying valid event or measurement values observed from a component .

An *observation* is a proposition in the form of $v_ij = d_jk$ which means the variable v_ij attains the *k-th* value d_jk in its domain D_j. Based on these concepts a system *state* can be uniquely specified by assigning different combinations of observations to all variables and write the state as $S := (v_{1i} = d_1) \vee \cdots \vee (v_{ni} = d_n)$. There are, hence, $\|D_s\| = \prod_{i=1}^{n} \|D_i\| = 0$ possible states.

An *action* is single system behavior, the occurrence of which triggers the system state to change from one state to another. Such behavior could be system inherent behavior, operator actions, attacks, or a clock timeout. An action is denoted as $A_l : S_i \rightarrow S_j$, where A_l causes the transition from S_i to S_j. Note that S_i and S_j can represent the same system state. This occurs when the expected response to an action does not occur. This would typically be an error condition.

An *event*, E_k, is a subset of state variables. The changes in the observations in these state variables are due to the corresponding action(s). An event alone with its corresponding actions is notated as $A_l E_k : S_i \rightarrow S_j$.

The $temporaldistance$ specifies the period of time between two states of a state transition. Temporal distance may be defined as a specific value or as a range such as $D = T_i - T_{i-1}$. Temporal distance may be defined as a specific value or as a range such as $D = T_i - T_{i-1} > 0$. Temporal distance from the root node is always 0 since the root node is system stable state and the second state is always the first evidence of a disturbance or attack.

The *path* is a sequence of signatures that describe a specific scenario. A *signature* contains a system state, its start time, actions and events, and temporal distance to the previous signature. A signature is formally represented as $\{S, T, Action \bigcap Event, D\}$. Once the path with temporal state transitions for the corresponding scenario ID is determined, the information in all signatures involved in the path is used to create the rule for our intrusion detection framework. We denote a path as $path = (Q_i, V, E, \eta)$ where Q_i is the path name which is the scenario name, V is a finite nonempty set of vertices/nodes, and $E = V \times V$ is a set of direct edges in the Bayesian network, and the function η is in the form of assigning observations to state variables, marking labels to each vertex. In this function, S is the name of this vertex, T is the start time of this vertex, $(Action \bigcap Event)$ is the label of this vertex and D is the temporal distance to previous vertex/vertecis.

The $Bayesiannetwork$ is composed of a number of paths. Therefore, it has the same composition as a path. We hence denote the Bayesian network as $\bigcup path_i = (Q_i, V, E, \eta_B)$, where $\eta_B(V) = \langle S, T, (Action \bigcap Event), Pr, D \rangle$. Note that the extra parameter Pr represents the conditional probability of the vertex. The construction of Bayesian network starts from the construction of a path. A path starts from an initial vertex standing for the system stable state. The expertise about the system under study e.g. knowledge about legitimate scenarios and threads is required when specifying the conditional probabilities. If the external impacts to our system are not considered, for example transmission errors in the telecommunication channel, it is reasonable to assign either 0 or 1 to each conditional probability so that all causal relationships become deterministic. And the action and event pair with its conditional probability of 1 will be used to mark the newly decided vertex. Paths propagate along with time until they distinct with each other

4.2 The Process of Constructing Bayesian Network for Over Current Protection Scheme

This section provides an overview of the process used to develop a Bayesian network for a set of scenarios (power system disturbances and cyber threats) which can occur for a given system. First, for a given system, a set of measurable variables are identified. Measured variables are system specific and are used to provide information about the system state. The list of measured variables is created by examining available data sources and comparing this with data needed to detect symptoms of set of scenarios. Quantized ranges are created for each measure variable to limit the state space. Domain expertise is required to list a set of possible actions which occur in the system. For each action a corresponding measurable event is identified. The actions are arcs in the Bayesian network which cause a state transition and the measurable events are evidence that the system has changed states. A Bayesian network is built by drawing a path through a set of system states which when connected describe a scenario. The goal of this process is to create a Bayesian network with a unique path for each scenario. When first drawn the Bayesian network paths may not be unique and overlapping occurs in the process in which the domain expert searches addition actions and events which when added allow each path to become unique. Once each scenario has a unique path the Bayesian construction process is complete and the paths for each scenario represent a measurable signature for each scenario.

4.2.1 Step 1 Identifies Measurable Variables or Events

The variables measured for the over current protection case study are relay operation state, presence of a remote command to trip the relay at the control room, presence of a remote command to trip the relay on the substation network as detected by Snort, and PMU current measurements from the bus connected to the relay.

Table 1: Component ranges

Component Name	Range
Line Current Magnitude	[**H**igh, **W**arning, **N**ormal, **Z**ero]
Snort log	[True, False]
Relay log	[True, False]
Control log	[True, False]

Operators need the ability to remotely trip a relay to remove a transmission line from the power system. Transmission lines are taken out of service to allow for maintenance. The presence of the trip command in the control room is either true or false as stated in Table 1. This measurement can be extracted from the human machine interface tool used by an operator to remotely trip the relay. For this work, this value was simulated. If the remote trip command was intended to be legitimate this value was set to true. If the remote trip command was illegitimate this value was set to false. Because a relay can be remotely tripped it is possible for an attacker to direct a spurious command to the relay to trip the relay without the knowledge or approval of system operators. In this case, the remote trip command will be seen on the substation network as it travels to the relay. For this work, a Snort signature was used to detect the presence of a remote trip command. This signature alerts for both legitimate and illegitimate remote trip commands and therefore is not enough information by itself to declare the presence of an attack. If the Snort signature detects a remote trip command this measurement is True and if a remote trip is not detected this measurement is false.

Relays which have operated open or close a contact connected to the breaker. This contact state is stored in the relay log file and the state of this contact can be read to learn the intended breaker status. This is the intended breaker status due to the possibility of breaker failure. We call this variable the relay status. Relay status is true if the relay has operated and false if the relay has not operated.

PMU can be used to measure a power system bus's voltage and current at rates up to 120 times per second. For this work a PMU was used to provide a measurement of current at the transmission line as a redundant indication of the transmission line status as well as whether the relay is opened or closed. The PMU measurement is a real number which can take a continuous set of values and therefore introduces an infinite number of states in the system state space. Such continuous measurements need to be quantized to a finite set of ranges. The current magnitude can range from zero to infinity. However, for the 2-generator 3-bus transmission system and the non-pilot directional over current protection scheme described previously, the PMU current can be broken into 4 ranges. The first range is over current which covers the case that the current exceeds the pickup of the relay. The instantaneous over current pickup for relay R2 in Figure 2 is set to 800 Amperes. The over current range is defined as [800 Ampere, Infinity) and denoted as "High". The second range is a warning range to allow for the case in which a fault occurs on an adjacent line which it is not cleared due to relay(s) failures. The warning range is hence below instantaneous over current pickup and above certain value. The minimum warning level current must be above a normal operating current when the system has maximum operating load. The current was measured within RSCAD by setting to operate at maximum load. Short circuit analysis was used to predict the short circuit current for a fault on adjacent lines. From these experiments in the test bed, we conclude the warning range is (600 Ampere, 800 Ampere).

The third range is the zero-magnitude range where current magnitude is relatively small. The zero current is not necessarily zero but is a relatively small value. For example, when relays R1 and R4 trip due to a fault on line L2, the current magnitude measured by the PMU at R2 is approximately 50 Amperes. Therefore, the zero-magnitude range for this test bed is defined as [0 Ampere, 60 Ampere). The fourth range is the normal range. The normal range is for current magnitudes above the zero range and below the warning range. For this case study the normal range is set to [60 Ampere, 600 Ampere). Table 2 shows the list of the permissible ranges of all measured variables in the test bed.

4.2.2 Step 2 Specifies Actions and Events which Describe System State Transitions

Table 2: Actions and event space

Action ID	Action	Event ID	Event
A0	Normal	E0	PMU = N, Relay log = F, Snort log =F, Control panel log = F
A1	Control panel sending tripping command	E1	PMU = H
A2	Fault in the line	E2	Control panel log = T
A3	Snort detecting tripping command	E3	Snort log = T
A4	Relay tripping	E4	Relay log = T
A5	Relay operating time out	E5	Relay log = F
A6	Injecting false data beyond the pickup	E1	PMU = H
A7	Injecting false data in permissible range	E6	PMU = N
A8	Injecting false data of zero magnitude	E7	PMU = Z
A9	Breaker opened	E7	PMU = Z
A10	Breaker failed	E8	PMU = H
A11	Fault in adjacent line	E9	PMU = W

The 10 scenarios previously described in the threat model section can be broken into series of actions and corresponding measurable events for each action. For the case study 12 actions and 10 corresponding events are identified. Identification of the actions and corresponding events requires domain expertise. Actions are actions which occur as part of a larger scenario. Actions cause system state to change. Measurable events are sensor measurements are values from log files which are indicative of a power system state. Measurable events are evidence of the system state. The concatenated action identifier and corresponding event identifier is unique to a system state and is therefore used to mark the states in the Bayesian network.

To create the action and corresponding events list the domain expert attempts to describe a set of actions which occur during a given scenario. For each action, the domain expert searches for a unique corresponding measurable event. It may not always be possible to identify a measurable event. It also may not be possible to identify a unique measurable event as seen by multiple actions in Table 2 which share the same event.

The action A10 represents a fault in an adjacent line. This action is used to allow scenarios from other lines to be classified and therefore to allow differentiation between scenarios occurring at the local relay and scenarios which occur at remote relays.

4.2.3 Step 3 Determines Paths for the Set of System Scenarios

A path is a set of system states arranged in temporal order. Each scenario is described by a path. All paths start from an initial state, the system stable state. For this case study the system stable state is the case in which the current magnitude, measured by the PMU, at line L1 is normal, the relay has not operated, the operator has not sent a remote trip command from the control room, and Snort has not detected a remote trip command on the substation network. This state is marked as action A0, event E0 or A0E0. The paths for system scenarios are described below as examples.

Scenario Q1 is an over current fault on line L1. The first action which occurs is the fault. The fault will be reflected by the current magnitude changing to the high state. This is measured by the PMU. This action and event pair is A1E1. The second action for scenario Q1 is the over current relay tripping. This is measured by reading the relay state from the relay log. This action and event pair is A4E4. The final action for scenario Q1 is the breaker is opened. This is evidenced by the event current magnitude changing to 0 Amperes which is measured by the PMU. This action and event pair is A9E7.

Scenario Q2 is transmission line L1 taken out of the power system for maintenance. The first action which occurs for this scenario is operator sends a remote command to trip the relay. This command is detected by reading the operators human machine interface log. This action and event pair is A2E2. The second action which occurs is the presence of the remote trip command in the substation communications network. This is detected by a Snort alert. This action and event pair is A3E3. The third action is the over current relay tripping. This is measured by reading the relay state from the relay log. This action and event pair is A4E4. The final action for scenario Q1 is the breaker is opened. This is evidenced by the event current magnitude changing to 0 Amperes which is measured by the PMU. This action and event pair is A9E7.

Scenario Q3 is a command injection attack which remotely trips the relay. The first action which occurs for this scenario is the presence of the remote trip command in the substation communications network. This is detected by a Snort alert. This action and event pair is A3E3. The third action is the over current relay tripping. This is measured by reading the relay state from the relay log. This action and event pair is A4E4. The final action for scenario Q1 is the breaker is opened. This is evidenced by the event current magnitude changing to 0 Amperes which is measured by the PMU. This action and event pair is A9E7.

The actions and events for a given path may occur simultaneously or may occur over a temporal distance. The temporal distance is defined as the time between action and event pairs or system states. Some paths have minimum or maximum temporal distance requirements. For example, if a fault occurs in line L1, relay R1 should trip in one cycle, then the breaker should open within the specified breaker operating time. Paths may have order requirements. This is specified by a temporal distance between an action and event pair or two states which is greater than 0.

4.2.4 Step 4 is Construction of the Bayesian Network with Temporal-state Transitions

A typical Bayesian network is represented as an acyclic directed graph (DAG) with a set of vertices and edges. The Bayesian network in this paper is distinct from traditional Bayesian networks in that its vertices contain a set of state variables, time, actions and events. An action and corresponding event pair (i.e. A#E#) is used to mark the vertices. The Bayesian network is constructed by graphing each path in temporal order. System states are represented on the Y-axis. As such a row on the graph will always have the same action and event pairs. The X-axis indicates time. Temporal distance between states or action and event pairs is shown by a path traveling from left to right on the graph. The X-axis unit is unlabeled because the different paths may have large temporal distance disparity. Therefore unit time is used to show order. The complete Bayesian network for all scenarios for relay R2 is shown in Figure 4.

In some cases the same action and event pair will lead to two different system states. For example, action and event pair A4E4 is show on two rows of the Bayesian network graph. In 3 cases the A4E4 action and event pair leads to system state S5 and on 1 case the same action and event pair leads to system state S4. The action and event pair represents a relay tripping and the resulting indication of such in the relay log. For state S5 this has occurred due to an over current fault. For state S5 this has occurred due to a command injection attack. The difference between these 2 states is that S5 has a high PMU current measurement and S4 has a normal PMU current measurement. Each path in the Bayesian network starts from the initial vertex T0S0 with label A0E0, which represents the system stable state.

The path includes all information needed for to build signatures for each scenario. The path can be used to describe the corresponding scenario by the sequences of actions and actions that cause the state transitions along with time. This Bayesian network consists 9 paths for 10 scenarios. Note that, scenarios Q5, Q6 and Q8, Q10 have the same paths. These paths contain leaf nodes, each of which has two possible actions. The two actions are mutually exclusive such that they cannot happen at the same time. However, at this stage there is not enough information to differentiate them. The extra information needed is the log from opposite relay on the same transmission line. For the scenario Q5 and Q6, if the over current is due to a fault in line L1 (A1E1), R1 will trip (R1 log = True) and open the breaker BR1 then the path will lead to scenario Q5. While in scenario Q6, the data injection (A5E5) does not cause relay R1 to trip therefore R1 log = False. Note that, this is also the case when distinguishing Q8 and Q9. The log information from relay R1 is needed again because the PMU in relay R2 reading zero current could implies two scenarios: one is due to a zero-value data injection attach (A8E7); the other results from the breaker being opened (A9E7) by the opposite relay R1. This second scenario belongs to the IDS monitoring the opposite relay, R1, and therefore is categorized as ”Other” by the IDS monitoring relay R2. The path Q10 represents scenarios which have occurred on an adjacent line or on the opposite relay on the same line. All paths in Figure 4 represent all possible scenarios that could happen in the test bed.

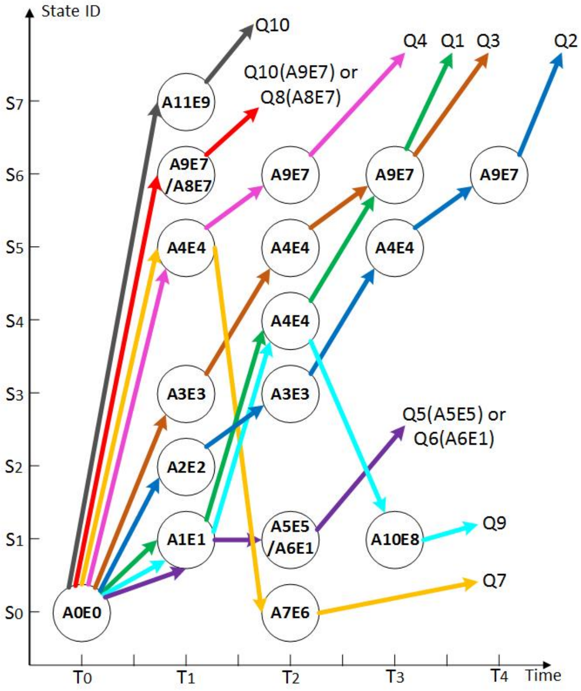

Figure 4: Complete Bayesian network for relay R2

4.3 Result and Discussion

An IDS was implemented from the Bayesian network shown in Figure 4. The IDS reads PMU current measurements, relay trip status, the snort log, and the control panel log and uses this information to track system states. The IDS monitors transitions from state to state to detect paths which match those shown in the Bayesian diagram. The result of the IDS was classification of the 10 scenarios. An experiment was conducted using the test bed shown in Figure 3. Scenarios Q1 to Q9 were simulated on a single transmission line of the 2-generator 3-bus transmission system. Line L1 and relay R2 were the target of all power system disturbances and or cyber attacks. Each scenario was reproduced 5 times; each time with a different load. Table 3 presents the results from the experiment. Each relay in the test bed included an embedded PMU. Time stamped PMU current, relay logs, Snort logs, and control panel logs were stored separately for each relay in the test bed. The IDS built from the Bayesian network graph in Figure 4 was used to post process data collected for each relay in the system and provide classification results.

Table 3 lists classification results from the experiment for each relay. The first column of Table 3 shows the scenario simulated. The next four columns show the classification result seen from the IDS when processing data associated with relays R1 to R4 respectively. Each scenario was run 5 times. The values in the cells of table III indicate the classified scenario or are labeled with a "-" if no classification result was generated for that scenario.

The results can be analyzed in 3 groups. First, IDS at the target relay, R2, always classified the scenarios correctly. The classification results for the IDS for R1 require explanation. First, scenario Q1 is an over current fault. Since the over current fault is seen by both relays on the line and both relays are programmed to respond to the fault instantaneously, the IDS classified this fault as Q1. This result is correct. Scenario Q2 simulates an operator taking line L1 out of service for maintenance. In this case the operator will remotely trip the relays R1 and R2 simultaneously. As such the IDS at R1 correctly classified these actions as scenario Q2. Scenarios Q3 and Q4 were classified as scenario Q10. Scenario Q10 is intended as a class which represents actions which occur at another relay. The intent of this work is to develop an IDS which monitors an atomic unit, a single relay, but ignores actions at other relays since these relays will have their own IDS. Scenario Q10 includes cases when the current at the relay, as measured by the PMU, enters the warning range, below the pickup current but above the normal range. Scenario Q10 also includes when the opposite breaker opens and the local PMU current drops to 0 Amperes without a previous current measurement greater than the pickup current setting. This second case occurs to one relay when its opposite relay trips. Scenario Q3 is a cyber attack in which a remote command is used to trip relay R2. In this case there is no longer a path for current from generator G1 to the load. This causes the current at relay R1 to drop to 0 Amperes without R1 first tripping which in turn causes the Q10 classification. Scenario Q4 is a physical attack in which a substation intruder or insider uses relay R2's face to trip relay R2 without permission. Again in this case there is not path for current to flow from generator G1 to the load and this leads to a Q10 classification. For scenarios Q3 and Q4 the Q10 classification is consider correct. Scenario Q5 is an over current fault in which relay R2 fails to operate. This missed operation may be due to relay failure or incorrect setting. In this case relay R1 operates correctly and trips due to the same over current fault on line L1. This is correctly classified as scenario Q1. Scenario Q6 and Q8 are not classified by the IDS at relay R1. This occurs because scenario Q6 and Q8 are two data injection attacks targeting the PMU at R2. Since this is a false PMU measurement the actual line current measured at relay R2 remains normal and the IDS at relay R1 sees no signature of a scenario. Scenario Q7 is a data injection attack which is attempting to mask an over current fault which causes relay R2 to trip. In this case there is a valid over current fault on the line and this fault is seen by relay R1. Since the data injection attack is limited to relay R2, relay R1's IDS correctly classifies this as scenario Q1. Finally, Q9 is an over current fault on line L1 with breaker failure at BR2. In this case there is a valid over current fault on the line and this fault is seen by relay R1. Since the breaker failure is limited to relay R2, relay R1's IDS correctly classifies this as scenario Q1.

The IDS(s) at relays R3 and R4 always classified scenarios as either Q10 or did not provide a classification at all. Scenarios Q1, Q5, Q7 and Q9 were all classified as scenario Q10. Each of these scenarios involve an over current fault on line L1. This fault on the neighboring line will cause the PMU current at relays R3 and R4 to read in the warning range which leads to this scenario Q10 classification. Scenarios Q2, Q3, and Q4 all involve relay R2 tripping without a prior fault. These cases may lead to a drop in current at R3 and R4. However, since there is another source in the power system, as is expected due to N-1 generator redundancy requirements, the current at R3 and R4 does not drop to 0 Amperes and therefore no signature of a Bayesian network path is available for classification. Scenarios Q6 and Q8 are data injection attacks which alter the PMU current measurement from relay R2. This has no effect on relays R3 and R4 and therefore there is no signature of a Bayesian network path classify. All of the classification results for relays R3 and R4 are considered correct.

4.4 Conclusion and Future Work

This paper introduces a methodology for developing specification based intrusion detection systems (IDS) for cyber-physical systems. The methodology involves first developing a threat model for the system to be monitored which includes relevant cyber attacks and any expected disturbances which may occur normally in the system. The threat model is grouped into a set of scenarios to be classified by the IDS. Next, a set of actions and measurable events is created for the system. The actions and events pair to move the system from state to state. A Bayesian network graph is constructed which shows each scenario as a path which describes system state transitions and temporal order for each path. In order to provide a unique classification for each scenario the Bayesian network graph must include a separate path for each scenario. IDS designers search for actions and measurable events in a loop until separate paths exist for each sce-

Table 3: Actions and event space

Scenario Simulated	Scenario Detected IDS@R1	Scenario Detected IDS@R2	Scenario Detected IDS@R3	Scenario Detected IDS@R4
Q1: Over current fault@L1	Q1	Q1	Q10	Q10
Q2: L1 removed for maintenance	Q2	Q2	-	-
Q3: command injection attack; remotely trip R2	Q10	Q3	-	-
Q4: physical attack; trip R2 at faceplate	Q10	Q4	-	-
Q5: fault@L1; relay does not trip	Q1	Q5	Q10	Q10
Q6: data injection attack IL1 > pickup	-	Q6	-	-
Q7: data injection attack; IL1<pickup; fault@L1	Q1	Q7	Q10	Q10
Q8: data injection attack; IL1=0	-	Q8	-	-
Q9: fault@L1; BR2 breaker failure	Q1	Q9	Q10	Q10

nario. Once the Bayesian event graph is complete an IDS can be built.

The proposed method for developing specification based IDS requires system expertise. This can be a burdensome requirement. A separate version of the IDS is deployed for each relay meaning the IDS does not need to consider attacks and disturbances which occur on a separate line. For this work the non-pilot directional over current relay protection scheme was specified. Other relaying schemes would also need to be specified. Each relay requires an instance of the IDS. IDS instances may be deployed in the substation at the relay location or a single server at a central location may run multiple instances of IDS to monitor multiple relays. The computing and networking resource requirements of both deployment options should be considered in future work. Other future work will the use of clustering algorithms [39, 41, 42] and game theory approaches to learn rules from observed behavior and game theory to better model interactions between system components before learning rules. Finally, the best approach to feature selection will be researched for various target systems [22].

For this work, a case study was used to demonstrate the effectiveness of the IDS development methodology. The case study was applied to the non-pilot directional over current relay protection scheme for a modified 2-bus 2-generator system taken from a section of the IEEE 9-bus 3-generator system. Nine scenarios were developed. The scenarios include 4 power system disturbance cases and 5 cyber attacks. A Bayesian network graph for the 9 scenarios was developed and data logs were captured for each scenario from the perspective of each relay in the test bed power system. The resulting IDS was used to post process data collected from perspective of each relay separately. All case study scenarios were correctly classified.

References

[1] U. Adhikari, T. H. Morris, N. Dahal, S. Pan, R. L. King, N. H. Younan, and V. Madani, "Development of power system test bed for data mining of synchrophasors data, cyber-attack and relay testing in rtds," in *2012 IEEE Power and Energy Society General Meeting*, pp. 1–7, July 2012.

[2] D. E. Bakken, A. Bose, C. H. Hauser, E. O. Schweitzer III, D. E. Whitehead, and G. C. Zweigle. "Smart generation and transmission with coherent, real-time data," Tech. Rep. TR-GS-015, School of Electrical Engineering and Computer Science, Washington State University, Jan. 2011.

[3] R. Berthier and W. H. Sanders, "Specification-based intrusion detection for advanced metering infrastructures," in *Dependable Computing (PRDC), 2011 IEEE 17th Pacific Rim International Symposium on*, pp. 184–193, Dec. 2011.

[4] W. L. Buntine, "A guide to the literature on learning probabilistic networks from data," *IEEE Transactions on Knowledge and Data Engineering*, vol. 8, pp. 195–210, Apr. 1996.

[5] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. N. Fovino, and A. Trombetta, "A multidimensional critical state analysis for detecting intrusions in scada systems," *IEEE Transactions on Industrial Informatics*, vol. 7, pp. 179–186, May 2011.

[6] A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," in *Pro-*

ceedings of the 3rd Conference on Hot Topics in Security, HOTSEC'08, pp. 6:1–6:6, 2008.

[7] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for securing cyber physical systems," in *Workshop on Future Directions in Cyber-physical Systems Security*, DHS, July 2009. [Online] Available: http://chess.eecs.berkeley.edu/pubs/601.html.

[8] E. Charniak, "Bayesian networks without tears," *AI Magazine*, vol. 12, no. 4, pp. 50–63, 1991.

[9] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes, "Using model-based intrusion detection for scada networks," in *Proceedings of the SCADA Security Scientific Symposium*, pp. 127–134, 2007.

[10] D. Dzung, M. Naedele, T. P. von Hoff, and M. Crevatin, "Security for industrial communication systems," *Proceedings of the IEEE*, vol. 93, pp. 1152–1177, June 2005.

[11] N. Falliere, L. O. Murchu, and E. Chien. "W32.stuxnet dossier,". tech. rep., Oct. 2010. [Online] Available: http://www.symantec.com/com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.

[12] U. S. Government Accountability Office (GAO). "Gao-11-117: Electricity grid modernization: Progress being made on cybersecurity guidelines, but key challenges remain to be addressed,". tech. rep., Jan. 2011.

[13] F. Geramiraz, A. S. Memaripour, and M. Abbaspour, "Adaptive anomaly-based intrusion detection system using fuzzy controller," *International Journal of Network Security*, vol. 14, pp. 352–361, Nov. 2012.

[14] A. Di Giorgio and F. Liberati, "Interdependency modeling and analysis of critical infrastructures based on dynamic bayesian networks," in *Control Automation (MED), 2011 19th Mediterranean Conference on*, pp. 791–797, June 2011.

[15] The Smart Grid Interoperability Panel Cyber Security Working Group. "Nistir 7628 guidelines for smart grid cyber security: Vol. 2, security architecture and security requirements,", Aug. 2010. [Online] Available: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.

[16] N. Hadjsaid, C. Tranchita, B. Rozel, M. Viziteu, and R. Caire, "Modeling cyber and physical interdependencies - application in ict and power grids," in *2009 IEEE/PES Conference on Power Systems Conference and Exposition (PSCE'09)*, pp. 1–6, March 2009.

[17] D. K. Holstein and J. Diaz, "Cyber security management for utility operations," in *the 39th Annual Hawaii International Conference on System Sciences (HICSS'06),* 2006.

[18] S. Horowitz, D. Novosel, V. Madani, and M. Adamiak, "System-wide protection," *IEEE Power and Energy Magazine*, vol. 6, pp. 34–42, Sep. 2008.

[19] S. H. Horowitz and A. G. Phadke, *Power System Relaying.* Wiley, 2008.

[20] http://openpdc.codeplex.com. *The Open Source Phasor Data Concentrator (OpenPDC).*

[21] E. O. Schweitzer III and H. J. Altuve, "Real-time synchrophasor applications for wide-area protection, control, and monitoring,", 2009. [Online] Available: https://www.selinc.com/WorkArea/DownloadAsset.aspx?id=6388.

[22] P. Kabiri and M. Aghaei, "Feature analysis for intrusion detection in mobile ad-hoc networks," *International Journal of Network Security*, vol. 12, pp. 42–49, Jan. 2011.

[23] U. B. Kjaerulff and A. L. Madsen, *Bayesian Network and Influence Diagrams, A Guide to Construction and Analysis*, Springer, 2012.

[24] C. Ko, M. Ruschitzka, and K. Levitt, "Execution monitoring of security-critical programs in distributed systems: a specification-based approach," in *1997 Proceedings of IEEE Symposium on Security and Privacy,* pp. 175–187, May 1997.

[25] F. R. Lin, C. H. Chiu, and S. C. Wu, "Using bayesian networks for discovering temporal-state transition patterns in hemodialysis," in *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'2002)*, pp. 1995–2002, Jan. 2002.

[26] H. Lin, A. Slagell, C. Di Martino, Z. Kalbarczyk, and R. Iyer, "Adapting bro into scada: Building a specification-based intrusion detection system for the dnp3 protocol," in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW'13)*, pp. 5:1–5:4, 2013.

[27] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS'09)*, pp. 21–32, 2009.

[28] V. Madami, M. Adamiak, and M. Thakur, "Design and implementation of wide area special protection schemes," in *Proceedings 2004 57th Annual Conference for Protective Relay Engineers*, pp. 392–402, Apr. 2004.

[29] C. Marinez, M. Parashar, J. Dyer, and J. Coroase. "Phasor data requirements for real time wide-area monitoring, control and protection applications,". tech. rep., 2005. [Online] Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.122.1737.

[30] M. Masera and I. N. Fovino, "Effects of intentional threats to power substation control systems," *International Journal of Critical Infrastructure*, vol. 4, no. 1-2, pp. 129–143, 2008.

[31] R. Mitchell and I. R. Chen, "Behavior rule based intrusion detection for supporting secure medical cyber physical systems," in *2012 21st International Conference on Computer Communications and Networks (ICCCN'2012)*, pp. 1–7, July 2012.

[32] Y. Mo, T. H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, pp. 195–209, Jan 2012.

[33] T. Morris, S. Pan, J. Lewis, J. Moorhead, N. Younan, R. King, M. Freund, and V. Madani, "Cybersecurity risk testing of substation phasor measurement units and phasor data concentrators," in *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW'11)*, pp. 24:1–24:1, 2011.

[34] R. Moxley and D. Dolezilek, "Case studies: Synchrophasors for wide-area monitoring, protection, and control," in *Proceedings of 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe)'2011*, pp. 1–7, Dec. 2011.

[35] National Energy Technology Laboratory (NETL). "A systems view of the modern grid,". tech. rep., U.S. Department of Energy (DOE), Jan. 2007.

[36] J. P. Nieto, L. E. Garza, M. Garza, and R. Morales, "Fault diagnosis of industrial systems with bayesian networks and neural networks," in *Proceedings of the 7th Mexican International Conference on Artificial Intelligence (MICAI'08)*, pp. 998–1008, 2008.

[37] P. Ning and S. Jajodia, *Intrusion Detection Techniques*, Wiley, 2004.

[38] Critical Infrastructure Protection (NAERC-CIP) North American Electric Reliability Corporation. "Nerc standardscip-002-4 through cip-009-4,", 2012. [Online] Available: http://www.nerc.com/page.php?cid=2—20.

[39] A. Patcha and J. M. Park, "A game theoretic formulation for intrusion detection in mobile ad hoc networks," *International Journal of Network Security*, vol. 2, pp. 131–137, March 2006.

[40] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, Morgan Kaufmann, 1988.

[41] Q. Quan, C. J. Xiao, and R. Zhang, "Grid-based data stream clustering for intrusion detection," *International Journal of Network Security*, vol. 15, pp. 1–8, Jan. 2013.

[42] Q. Quan, T. Wang, and R. Zhan, "Relative network entropy based clustering algorithm for intrusion detection," *International Journal of Network Security*, vol. 15, pp. 16–22, Jan. 2011.

[43] M. F. Raihan and M. Zulkernine, "Detecting intrusions specified in a software specification language," in *29th Annual International Conference on Computer Software and Applications (COMPSAC'2005)*, vol. 1, pp. 143–148, July 2005.

[44] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems*, vol. 21, pp. 11–25, Dec. 2001.

[45] P. Sauer and A. Pai, *Power System Dynamics and Stability*, Stipes Publishing Co., 2007.

[46] R. Sprabery, T. Morris, S. Pan, U. Adhikari, and V. Madani, "Protocol mutation intrusion detection for synchrophasor communications," in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW'13)*, pp. 41:1–41:4, 2013.

[47] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, pp. 210–224, Jan. 2012.

[48] IEEE Standard, "IEEE standard for synchrophasor data transfer for power systems," *IEEE Std C37.118.2-2011 (Revision of IEEE Std C37.118-2005)*, pp. 1–53, Dec. 2011.

[49] M. Uddin, A. A. Rehman, N. Uddin, J. Memon, R. Alsaqour, and S. Kazi, "Signature-based multi-layer distributed intrusion detection system using mobile agents," *International Journal of Network Security*, vol. 15, pp. 97–105, Jan. 2013.

[50] P. Uppuluri and R. Sekar, "Experiences with specification-based intrusion detection," in *Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID'00)*, pp. 172–189, 2001.

[51] www.snort.org. *Snort.*

[52] Y. Liu and H. Man, "Network vulnerability assessment using bayesian networks," in *Proceedings of SPIE - Data Mining, Intrusion Detection, Information Assurance and Data Networks Security (SPIE'05)*, pp. 61–71, 2005.

[53] Z. Yongli, H. Limin, and Lu Jinling, "Bayesian networks-based approach for power systems fault diagnosis," *IEEE Transactions on Power Delivery*, vol. 21, pp. 634–639, Apr. 2006.

[54] Z. Zhang, H. Shen, and Y. Sang, "An observation-centric analysis on the modeling of anomaly-based intrusion detection," *International Journal of Network Security*, vol. 4, pp. 292–305, May 2007.

[55] C. Zimmer, B. Bhat, F. Mueller, and S. Mohan, "Time-based intrusion detection in cyber-physical systems," in *Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS'10)*, pp. 109–118, 2010.

[56] J. Zuo, R. Carroll, P. Trachian, J. Dong, S. Affare, B. Rogers, L. Beard, and Y. Liu, "Development of tva superpdc: Phasor applications, tools, and event replay," in *Proceedings of 2008 IEEE Conference on Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, pp. 1–8, July 2008.

Shengyi Pan received the B.Eng. degree from Fuzhou University, China, in 2008 and the M.S. degree from University of Sheffield, U.K., in 2009. He is currently working toward the Ph.D. degree in Mississippi State University, Mississippi State. His research interests include security and intrusion detection for computer network, process control system, and smart grid.

Thomas Morris received the Ph.D. degree from Southern Methodist University, Dallas, TX, in 2008. He currently serves as Associate Professor of Electrical and Computer Engineering at Mississippi State University, Mississippi State, MS, USA. His research interests include industrial control system penetration testing and intrusion detection systems.

Uttam Adhikari received the B.S. degree in electrical engineering from Tribhuvan University, Nepal, in 2005, and is currently pursuing graduate studies at Mississippi State University, Mississippi State. His research interests include wide area monitoring, control, and cyber security in smart grid.