Behavior-Rule Based Intrusion Detection Systems for Safety Critical Smart Grid Applications

Robert Mitchell and Ing-Ray Chen, *Member, IEEE*

***Abstract*—In this paper, a behavior-rule based intrusion detection system (BRIDS) is proposed for securing head-ends (HEs), distribution access points/data aggregation points (DAPs) and subscriber energy meters (SEMs) of a modern electrical grid in which continuity of operation is of the utmost importance. The impact of attacker behaviors on the effectiveness of a behavior-rule intrusion detection design is investigated. Using HEs, DAPs and SEMs as examples, it is demonstrated that a behavior-rule based intrusion detection technique can effectively trade false positives for a high detection probability to cope with sophisticated and hidden attackers to support ultra safe and secure applications. It is shown that BRIDS outperforms contemporary anomaly-based IDSs via comparative analysis.**

***Index Terms*—Cyber physical systems, data aggregation point, distribution access point, head-end, intrusion detection, safety, security, subscriber energy meter.**

I. Introduction

THE most prominent characteristic of a smart grid such as a modern electrical grid or electricity infrastructure is the feedback loop that acts on the physical environment. In other words, the physical environment provides data to the sensors attached to the Wide Area Networks (WANs), Neighborhood Area Networks (NANs) and Home Area Networks (HANs) whose data feed the control units in the production, transmission, distribution and consumption segments that drive the actuators which change the physical environment. Modern electricity infrastructure is often characterized by sophisticated reliability, efficiency, sustainability and utility control units interacting with the physical environment including subscriber appliances. This paper concerns intrusion detection mechanisms for detecting compromised devices embedded in WANs, NANs and HANs for supporting safe and secure applications that subscribers can depend on with confidence.

Intrusion detection system (IDS) techniques for this domain are still in their infancy with very little work reported in the literature. Only [2], [3], [6], [10], [13], [14], [16], [19]–[23] reported related intrusion detection. However, nine of these had no numerical data regarding the false negative probability p_{fn} (i.e., missing a bad node) and the false positive probability p_{fp} (i.e., misidentifying a good node as a bad node). The other three had minimal numerical data: one or two data points characterizing $p_{\mathrm{fn}}/p_{\mathrm{fp}}$ instead of a dataset that could be transformed into a *Receiver Operating Characteristic* (ROC) plot, i.e., a p_{fn} versus p_{fp} curve that describes the relationship between p_{fn} and p_{fp} obtained as a result of applying IDS techniques.

Specifically, Zhang *et al.* [22], [23] studied two detection algorithms called CLONALG and AIRS2Parallel. CLONALG is unsupervised. AIRS2Parallel is semi-supervised. They reported that CLONALG had a detection accuracy between 80.1% and 99.7% and AIRS2Parallel had an accuracy between 82.1% and 98.7%, where the detection accuracy is the likelihood that a node is classified correctly, calculated by $1 - p_{\mathrm{fp}} - p_{\mathrm{fn}}$. He and Blum [10] investigated a series of anomaly-based IDSs including Locally Optimum Unknown Direction (LOUD), Locally Optimum Estimated Direction (LOED), LOUD-Generalized Likelihood Ratio (LOUD-GLR) and LOED-Generalized Likelihood Ratio (LOED-GLR). He and Blum's LOUD-GLR approach performed the best: The maximum detection rate (i.e., $1 - p_{\mathrm{fn}}$) is reportedly 95%. However, no ROC data were given in [10], [22], [23].

Intrusion detection techniques in general can be classified into three types: signature-based, anomaly-based and specification-based techniques. In this paper, specification-based detection is considered rather than signature-based detection to deal with unknown attacker patterns. Specification-based techniques are considered rather than anomaly-based ones (such as those by Zhang *et al.* [22], [23] and He and Blum [10]) to avoid using resource constrained sensors or actuators in a WAN for profiling anomaly patterns (for example, through learning) and to avoid high false positives (treating good nodes as bad nodes).

To accommodate resource constrained devices, this paper develops the design notion of behavior rules for specifying acceptable behaviors of physical devices in a WAN, NAN or HAN. Rule-based intrusion detection thus far has been applied only in the context of communication networks which have no concern of physical environments and the closed-loop control structure as in a head-end (HE), distribution access point/data aggregation point (DAP) or subscriber energy meter (SEM).

In the literature, specification-based IDS techniques have been proposed for intrusion detection of communication protocol misbehaving patterns [7]–[9], [12]. Da Silva *et al.* [8] propose an IDS that applies seven types of traffic-based rules to detect intruders: interval, retransmission, integrity, delay, repetition, radio transmission range and jamming. Ioannis *et al.* [12] propose a multitrust IDS with traffic-based collection that audits the forwarding behavior of suspects to detect blackhole and greyhole attacks launched by captured devices based on the the rate (versus the count) of specification violations. [7], [9] also only considered specification-based state

Manuscript received August 18, 2012; revised November 29, 2012, January 10, 2013, and March 31, 2013; accepted April 15, 2013. Date of publication April 29, 2013; date of current version August 21, 2013.

The authors are with the Department of Computer Science, Virginia Polytechnic Institute and State University, Falls Church, VA 22043 USA (e-mail: rrmitche@vt.edu; irchen@vt.edu).

Digital Object Identifier 10.1109/TSG.2013.2258948

machines for intrusion detection of misbehaving patterns in communication networks. The specification-based technique in this paper distinguishes itself from [7]–[9], [12] cited above by addressing the unique requirements of the domain. First, modern electricity infrastructure has control loops that tie the physical environment to the CPS. Second, components are stationary which eliminates IDSs based on instantaneous motion or movement profiles. Third, they are federated systems; bulk power generators, energy markets, transmission providers, distribution providers and subscribers own, host and operate different segments of the CPS. Fourth, their scale is substantial; for example, the count of SEMs could be in the millions. Fifth, these CPSs are heterogeneous. In this work, specification-based behavior rules are derived from control loops which tie the intrusion detection to the critical business rules of the CPS while not relying on motion or track data used in other approaches. Also, the goals of each interest in the CPS are considered in forming behavior rules: bulk power generators want full utilization, energy markets want to match supply and demand, micro grids want to optimize sustainability or reliability and customers want to minimize cost. To address scalability, the state machines are pruned and tunable audit frequencies are provided. Three node types are considered to account for heterogeneity in the CPS.

The contribution of our work relative to prior work cited is that behavior rules for WAN, NAN and HAN devices controlling actuators and sensors embedded in the physical environment are specifically considered. Further, a method to transform behavior rules to a state machine is proposed, so that a device that is being monitored for its behavior can be checked against the transformed state machine for deviation from its behavior specification. Untreated in the literature [17], in this paper the impact of attacker behaviors on the effectiveness of intrusion detection in the production, transmission, distribution and consumption segments is also investigated. Using HEs, DAPs and SEMs as examples, it is demonstrated that an intrusion detection technique can effectively trade false positives for a high detection probability to cope with more sophisticated and hidden attackers to support ultra safe and secure applications. Moreover, it is shown that a behavior-rule based intrusion detection system (BRIDS) design outperforms contemporary anomaly-based IDSs [10], [22], [23] via comparative analysis.

II. Model and Design

A. System Model

1) Reference System: A modern electrical grid cyber physical system (CPS) embedding physical components is considered as the reference model as illustrated in Fig. 1. For ease of disposition, this paper is particularly concerned with three types of physical devices: HEs, DAPs and SEMs. Many examples exist with these three devices. Fig. 1 shows their hierarchical relationship: The scope of an HE, which is operated by a bulk power generator or energy market, encompasses many DAPs, which are operated by the transmission or distribution providers. The scope of a DAP encompasses many SEMs, which are hosted by subscribers (residential, commercial or industrial). This figure also shows the control modules running at each node: Host and system IDS modules run on every HE, DAP and SEM. Host IDS modules are loaded with the state machines pertaining to the relevant trustees. For example, HE host IDSs include HE and DAP state machines while SEM host IDSs include SEM and DAP state machines. Fig. 1 illustrates the control modules, actuators and sensors that relate to the IDS design and how it integrates with the existing communications infrastructure. Power Line Communication links HEs to DAPs, IEEE 802.11s Wireless Mesh Networking links DAPs to SEMs and IEEE 802.15.4 Wireless Personal Area Networking links SEMs to smart appliances and customer distributed energy resources (DERs). DERs are alternatives to the bulk power generators. Including capital investment, fuel and consumables for both, the cost per Watt for DERs is typically higher. However, DERs (e.g., wind generators, geothermal units or solar cells) surpass bulk power generators (e.g., coal or nuclear-powered) in sustainability. While they are not advantageous in terms of sustainability, hydrocarbon-based (in addition to the renewable) DERs provide redundancy in case of breakage in the transmission network. Members of a micro grid can pool resources to buy and operate a community DER or individual subscribers can go it alone. A database collects, stores and distributes data from sensors. A human machine interface (HMI) allows an operator to control the system and view its status using sensor data in the colocated database. Fig. 1 shows two actuators for the HE: a bulk generator and isolation switches. The bulk generator may come in the form of a large-capacity power station consuming hydrocarbon or fissile fuel. Isolation switches open and close circuits in the transmission network due to faults or maintenance. Fig. 1 shows two actuators for the DAP: an islanding switch and a community DER. The islanding switch separates and joins a micro grid with the transmission network due to faults or maintenance. A community DER may come in the form of a medium-scale wind generator, geothermal unit or solar cell array. Fig. 1 shows two actuators for the SEM: a smart appliance and a subscriber DER. A smart appliance tailors its duty cycle (e.g., compressor active/idle ratio for an HVAC unit) or scheduling (e.g., start time for a dishwasher) based on micro grid demand and billing rate. A community DER may come in the form of a small-scale wind generator, geothermal unit or solar cell array. Fig. 1 shows two sensors for each of the HE, DAP and SEM which detect demand (Watts) and faults (derived from phase of the AC waveform) at the system, micro grid and subscriber levels, respectively.

2) Behavior Monitoring: Our IDS approach is based on behavior monitoring. A neighbor HE, DAP or SEM is used to monitor (specifically, measure the compliance degree of) one or more trustees of different types. DAPs are less resource rich than an HE due to high volume and tight size, weight and power constraints. However, they are plentiful which results in significant aggregate time and space that can be accumulated to monitor other DAPs or SEMs. An SEM monitors other neighboring SEMs only due to a high degree of resource constraints.

3) Threat Model: The threat model explains possible attacks performed by a compromised device (HE, DAP or SEM), which will cause its behavior to deviate from good behaviors specified by a set of behavior rules used by the IDS. Two attacker archetypes are differentiated: reckless and random. A reckless attacker performs attacks whenever it has a chance. The main objective is to impair the functionality at the earliest possible time. A random attacker, on the other hand, performs attacks only randomly to avoid detection. It is thus insidious and deceptive with the objective to cripple the functionality. The attacker behavior is modeled by a random attack probability p_a. When $p_a = 1$ the attacker is a reckless adversary. Imperfect monitoring is modeled by an error parameter, p_{err}, representing the probability of a monitor node misidentifying the status of the trustee node due to ambient noise, temporary system faults, and/or wireless communication faults in the environment. In general a node may deduce p_{err} at runtime by sensing the amount of ambient noise, system errors, and/or wireless communication errors around it.

B. Problem Definition

We define the problem to be solved in the context of Fig. 1. Broadly, the problem we are trying to solve is the vulnerability to infrastructure damage, service interruption and revenue loss caused by malicious actors. We aim to provide a solution to this problem by detecting malicious devices that exploit the vulnerability through known or unknown attacks. The solution we are offering is a behavior-rule based design with which misbehavior of a device manifested as a result of attacks exploiting the vulnerability exposed may be detected, regardless of whether the attack is known or unknown. In the context of the electrical power grid in Fig. 1, we aim to solve this problem by detecting malicious devices, including HE, DAP and SEM devices. For example, an opportunistic vandal could completely unfurl the blades of a wind DER during high wind conditions to damage the apparatus. A state sponsored attacker could open the isolation switches at a bulk energy provider to disrupt the service to the utilitys customers. A disgruntled insider at a bulk energy provider could lower the billing rate to cause the enterprise to lose money on all power it sold at the artificially depressed rate. A frugal subscriber could modify the usage reporting module of their subscriber energy meter to reduce their financial obligation to the energy provider. Regardless of the form of attacks, we aim to provide a solution for malicious device detection that is accurate in detection rate (close to 100%) while limiting the false positive probability to a minimum (e.g., less than 10%).

C. Behavior Rules

Our IDS design for the reference model relies on the use of lightweight specification-based *behavior rules* for each device. They are oriented toward detecting an inside attacker attached to a specific physical device, providing a continuous output between 0 and 1 (while accounting for transient faults and human errors) and allowing a monitor to perform intrusion detection on a neighbor trustee through monitoring. Here a monitor is itself a physical device with capability to do intrusion detection on trustee nodes assigned to it. For example, an SEM may monitor another SEM within radio range. An HE may monitor other HE or DAP trustee devices within radio range. Therefore, an HE might have several sets of behavior rules (and thus several state machines), one for each trustee.

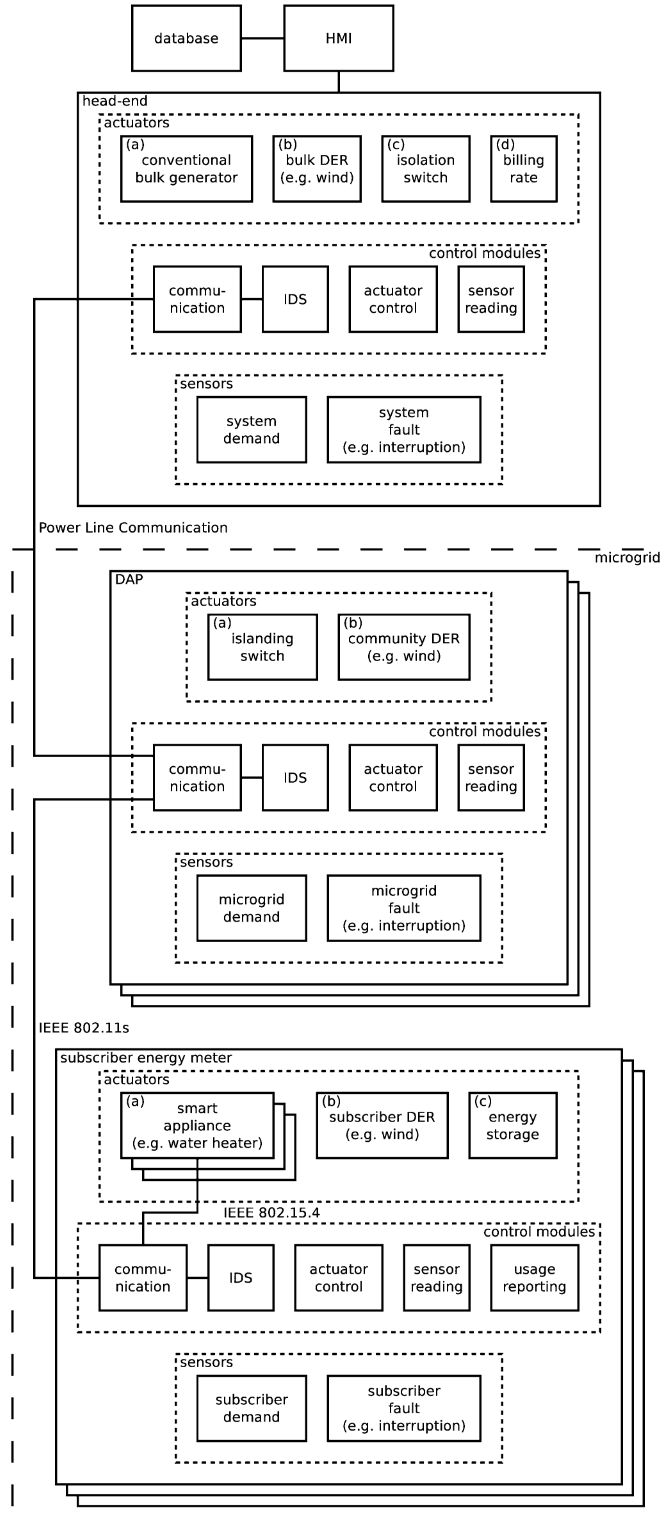

Fig. 1. Modern electrical grid CPS.

Tables I, II and III list the behavior rules for the HE, DAPs and SEMs. These tables specify the trustee and monitor devices for applying the IDS technique.

The networking concepts used in the behavior rules include: *Packets received* are the inbound protocol data units handled by the communications subsystem or application on a node; they are measured with frequency (Hz) with a domain of 0 to

TABLE I
HE BEHAVIOR RULES

Description	Trustee	Monitor
Turn off appliance block (for example, all water heaters in a microgrid) if system demand is above threshold	HE	HE
Decrease duty cycle (t/T, where t = pulse width and T = period) for appliance block if system demand is above threshold	HE	HE
Turn on appliance block if system demand is below threshold	HE	HE
Increase duty cycle (t/T, where t = pulse width and T = period) for appliance block if system demand is below threshold	HE	HE
Increase billing rate if system demand is above threshold	HE	HE
Decrease billing rate if system demand is below $\mu_d - \epsilon_d$	HE	HE
Close isolation switch if no fault or maintenance	HE	HE
Connect DER to distribution segment if system demand is above $\mu_d + \epsilon_d$	HE	HE
If fault sensors indicate an interruption, notify affected nodes	HE	HE

TABLE II
DAP BEHAVIOR RULES

Description	Trustee	Monitor
Request subscriber load decrease if subscriber demand is above $\mu_d + \epsilon_d$	DAP	DAP, HE
Request subscriber load increase if subscriber demand is below $\mu_d - \epsilon_d$	DAP	DAP, HE
Open island switch if bulk generation is interrupted	DAP	DAP, HE
Relay packets	DAP	DAP, HE
Don't source (replay or inject) packets	DAP	DAP, HE
Use community DER generators if available	DAP	DAP, HE
If fault sensors indicate an interruption, notify affected nodes	DAP	DAP, HE
If demand above threshold, increase pitch of (unfurl) wind DER generator to maximize power	DAP	DAP, HE
If demand below threshold, decrease pitch of (furl) wind DER generator to maximize lifetime	DAP	DAP, HE

TABLE III
SEM BEHAVIOR RULES

Description	Trustee	Monitor
Generate usage data periodically	SEM	SEM, DAP
Deactivate time independent appliances if billing rate is above $\mu_r + \epsilon_r$	SEM	SEM, DAP
Activate time independent appliances or store energy if billing rate is below $\mu_r - \epsilon_r$	SEM	SEM, DAP
Deactivate time independent appliances if microgrid demand is above $\mu_d + \epsilon_d$	SEM	SEM, DAP
Activate time independent appliances or store energy if microgrid demand is below $\mu_d - \epsilon_d$	SEM	SEM, DAP
Use subscriber DERs if available	SEM	SEM, DAP
If fault sensors indicate an interruption, notify affected nodes	SEM	SEM, DAP
If subscriber demand above threshold, increase pitch of (unfurl) wind DER generator to maximize power	SEM	SEM, DAP
If subscriber demand below threshold, decrease pitch of (furl) wind DER generator to maximize lifetime	SEM	SEM, DAP

10 packets per second. A node receives packets for which it is not the intended receiver, but possibly is a waypoint on the path to the destination. The communications subsystem drops these packets or relays them. *Packets forwarded* counts these packets the communications subsystem passes along using frequency (Hz) over the same domain as packets received. *Packet sourcing* is when an application generates a protocol data unit and passes it down to the communications subsystem for transmission. A good node populates these packets with legitimate sensor or status data, but a bad node populates these packets with corrupt sensor or status data or replays of previously received packets. ϵ_f is a threshold for the difference between packets received and packets forwarded. The *networking condition* is an abbreviation of packets received and forwarded used to manage the size of the behavior rule state machine. μ_d is the nominal power demand. ϵ_d is a distance from μ_d beyond which a control algorithm should take action to match power supply with demand. μ_r is the nominal billing rate. ϵ_r is a distance from μ_r beyond which a control algorithm should take action to capitalize on a low billing rate or avoid consuming at a high one.

Our behavior-rule specification-based technique approaches the intrusion detection problem from the behavior/evidence domain compared with signature-based techniques that approach the problem from the attacker domain. Hence, the patterns by which an attacker performs attacks and "how" an attacker performs attacks do not need to be known. Rather, a monitor device simply checks the behavior of a trustee device manifested from evidence of compliance/deviation against "good" and "bad" behaviors specified by a set of behavior rules for that device. Our approach thus can address all potential attacks, known or unknown. We claim behavior rule-based detection is able to cope with unknown attacks because all attacks lead to behavior anomaly. This capability is similar to anomaly detection which, unlike signature-based detection, can cope with zero-day attacks. Nevertheless, if the rule set is incomplete, that is, if the specification of anticipated behavior is incomplete, it is possible misbehavior manifested as a result of known or unknown attacks will be missed, and, consequently, the attacker will be undetected.

D. *Transforming Rules to State Machines*

Each behavior rule does not specify just one attack state, but a number of states, some of which are good states in which good behavior (obedience of this behavior rule) is observed, while others are bad states in which bad behavior (violation of this behavior rule) is observed. A behavior rule thus has a number of state variables, each with a range of values, together indicating whether the node is in good or bad behavior status (with respect to this rule). A device (HE, DAP or SEM), on the other hand, has a number of behavior rules; thus, it is possible that the state variables for one rule have intersections with those in another rule if they have the same logical clause. For example, the "system demand" state variable appears in HE rules 1–5 and 7. In this case, only one state variable will be used in these six rules to represent the "system demand" status. At the end, the underlying state machine for the behavior rule set of a device (e.g., Table I for HE) will consist of a set of unique state variables common to all behavior rules (e.g., system demand in HE rules 1–5 and 7) together indicating whether a device is in a good or bad behavior state (reflecting all behavior rules).

The following procedure transforms a behavior specification into a state machine: First, the "bad behavior indicator" as a result of a behavior rule being violated is identified. Then, this bad behavior indicator is transformed into a conjunctive normal form predicate and the involved state components in the underlying state machine are identified. Next, for each device (that is, an HE, DAP or SEM), the bad behavior indicators are combined into a Boolean expression in disjunctive normal form. Then, the union of all predicate variables is transformed into the state components of a state machine and their corresponding ranges are established. Finally, the number of states is managed by state collapsing and identifying combinations of values that are not legitimate. How a state machine is derived from the behavior specification in terms of behavior rules for the reference model is exemplified below.

1) Identify Bad Behavior Indicators: Attacks performed by a compromised sensor/actuator will drive the HE, DAP or SEM into certain bad behavior indicators identifiable through analyzing the specification-based behavior rules.

For the HE device, there are nine bad behavior indicators as a result of violating the nine behavior rules for HEs listed in Table I. The first HE bad behavior indicator is that the HE activates a block of appliances but the system demand is above some threshold. The second HE bad behavior indicator is that the HE increases the duty cycle for a block of appliances but the system demand is above some threshold. The third HE bad behavior indicator is that the HE deactivates a block of appliances but the system demand is below some threshold. The fourth HE bad behavior indicator is that the HE decreases the duty cycle for a block of appliances but the system demand is below some threshold. The fifth HE bad behavior indicator is that the HE decreases the billing rate but the system demand is above some threshold. The sixth HE bad behavior indicator is that the HE increases the billing rate but the system demand is below some threshold. The seventh HE bad behavior indicator is that the HE opens the switch for a micro grid but there is no associated fault or maintenance. The eighth HE bad behavior indicator is that DERs are disconnected but the system demand is above some threshold. The ninth HE bad behavior indicator is that an interruption is present but the HE has not generated an alert. For all of these HE bad behavior indicators, the HE is the trustee and all DAPs are monitors.

For the DAP device, there are eight bad behavior indicators as a result of violating the nine behavior rules for DAPs listed in Table II. The first DAP bad behavior indicator is that the HE requests a load increase, but micro grid demand is above some threshold. The second DAP bad behavior indicator is that the HE requests a load decrease, but micro grid demand is below some threshold. For these first two DAP bad behavior indicators, the HE is the trustee, and a DAP is the monitor. The third DAP bad behavior indicator is that the micro grid is islanded, but there is no interruption. For the third DAP bad behavior indicator, a DAP is the trustee, and the HE is the monitor. The fourth DAP bad behavior indicator is that the number of packets forwarded by the DAP does not equal the number of packets received by the DAP. This rule corresponds with the two behavior rules concerning packet handling. For the fourth DAP bad behavior indicator, a DAP is the trustee, and the HE and SEMs are monitors. The fifth DAP bad behavior indicator is that the community DER is not connected, but it is available. The sixth DAP bad behavior indicator is that an interruption is present, but the DAP has not generated an alert. The seventh DAP bad behavior indicator is that the DAP decreases the pitch of wind DER generator blades, but the micro grid demand is above some threshold. The eighth DAP bad behavior indicator is that the DAP increases the pitch of wind DER generator blades, but the micro grid demand is below some threshold. For the fifth through eighth DAP bad behavior indicators, a DAP is the trustee, and the HE is the monitor.

TABLE IV
HE Bad Behavior Indicators in Conjunctive Normal Form

(Appliance Block = ACTIVE) $\wedge$ (System Demand $> \mu_d + \epsilon_d$)
(New Appliance Duty Cycle $>$ Old Appliance Duty Cycle) $\wedge$ (System Demand $> \mu_d + \epsilon_d$)
(Appliance Block = INACTIVE) $\wedge$ (System Demand $< \mu_d - \epsilon_d$)
(New Appliance Duty Cycle $<$ Old Appliance Duty Cycle) $\wedge$ (System Demand $< \mu_d - \epsilon_d$)
(New Billing Rate $<$ Old Billing Rate) $\wedge$ (System Demand $> \mu_d + \epsilon_d$)
(New Billing Rate $>$ Old Billing Rate) $\wedge$ (System Demand $< \mu_d - \epsilon_d$)
(Isolation Switch Position = OPEN) $\wedge$ (Fault = FALSE) $\wedge$ (Maintenance = FALSE)
(DER = DISCONNECTED) $\wedge$ (System Demand $> \mu_d + \epsilon_d$)
(Interruption = TRUE) $\wedge$ (Alert = NULL)

For the SEM device, there are nine bad behavior indicators as a result of violating the nine behavior rules for SEMs listed in Table III. The first SEM bad behavior indicator is that the SEM is not generating usage data. The second SEM bad behavior indicator is that time-independent smart appliances are active, but the billing rate is above some threshold. The third SEM bad behavior indicator is that the subscriber is not banking electricity, but the billing rate is below some threshold. The fourth SEM bad behavior indicator is that time-independent smart appliances are active, but the demand is above some threshold. The fifth SEM bad behavior indicator is that the subscriber is not banking electricity, but the demand rate is below some threshold. The sixth SEM bad behavior indicator is that the subscriber DER is not connected, but it is available. The seventh SEM bad behavior indicator is that an interruption is present, but the SEM has not generated an alert. The eighth SEM bad behavior indicator is that the SEM decreases the pitch of wind DER generator blades, but the subscriber demand is above some threshold. The ninth SEM bad behavior indicator is that the SEM increases the pitch of wind DER generator blades, but the subscriber demand is below some threshold. For all of these SEM bad behavior indicators, an SEM is the trustee, and the DAP is the monitor.

2) Express Bad Behavior Indicators in Conjunctive Normal Form: Tables IV, V and VI list the bad behavior indicators in Conjunctive Normal Form for HE, DAP and SEM nodes, respectively.

3) Consolidate Predicates in Disjunctive Normal Form: Each type of device (HE, DAP or SEM) has a distinct behavior rule set based on its specific control modules, actuators and sensors. Construct the DNF predicate for each device type by joining the corresponding Tables IV, V or VI expressions with a disjunction. For clarity, the DNF predicate was left unreduced; clauses in the DNF predicate are traced to behavior rules easily. This makes it evident that attacks interact through

TABLE V
DAP BAD BEHAVIOR INDICATORS IN CONJUNCTIVE NORMAL FORM

(New Load Request $>$ Old Load Request) $\wedge$ (Microgrid Demand $> \mu_d + \epsilon_d$)
(New Load Request $<$ Old Load Request) $\wedge$ (Microgrid Demand $< \mu_d - \epsilon_d$)
(Island Switch Position = OPEN) $\wedge$ (Interruption = TRUE)
$\lvert$Forwarded Packets - Received Packets$\rvert > \epsilon_f$
(DER Connection = FALSE) $\wedge$ (DER Availability = TRUE)
(Interruption = TRUE) $\wedge$ (Alert = NULL)
(New Pitch $<$ Old Pitch) $\wedge$ (Microgrid Demand $> \mu_d + \epsilon_d$)
(New Pitch $>$ Old Pitch) $\wedge$ (Microgrid Demand $< \mu_d - \epsilon_d$)

TABLE VI
SEM BAD BEHAVIOR INDICATORS IN CONJUNCTIVE NORMAL FORM

Time $>$ Usage.Timestamp + ϵ
(Appliance = ACTIVE) $\wedge$ (Billing Rate $> \mu_r + \epsilon_r$)
(Energy Storage = FALSE) $\wedge$ (Billing Rate $< \mu_r - \epsilon_r$)
(Appliance = ACTIVE) $\wedge$ (Microgrid Demand $> \mu_d + \epsilon_d$)
(Energy Storage = FALSE) $\wedge$ (Microgrid Demand $< \mu_d - \epsilon_d$)
(DER Connection = FALSE) $\wedge$ (DER Availability = TRUE)
(Interruption = TRUE) $\wedge$ (Alert = NULL)
(New Pitch $<$ Old Pitch) $\wedge$ (Subscriber Demand $> \mu_d + \epsilon_d$)
(New Pitch $>$ Old Pitch) $\wedge$ (Subscriber Demand $< \mu_d - \epsilon_d$)

TABLE VII
MODERN ELECTRICITY INFRASTRUCTURE STATE COMPONENTS

Name	Control or Reading	Range
Appliance Block Activation	Control	true, false
System Demand	Reading	[0, 1000 GW]
Appliance Duty Cycle	Control	[0, 100%]
Billing Rate	Control	(0, 1 USD/kWh]
Switch Position	Control	open, closed
Fault	Reading	false, true
Maintenance	Control	false, true
DER Connection	Control	false, true
Interruption	Reading	false, true
Alert	Control	false, true
Load Request	Control	[0, 1000 kW]
Microgrid Demand	Reading	[0, 1000 MW]
Island	Control	false, true
Forwarded Packets	Reading	[0, 10/s]
Received Packets	Reading	[0, 10/s]
DER Availability	Reading	false, true
Wind DER Generator Pitch	Control	[0, 90°]
Usage Age	Reading	[0, 2^{32}]
Appliance Activation	Control	false, true
Energy Storage	Control	false, true
Subscriber Demand	Reading	[0, 1000 kW]

common state variables with the same logical clause. While it will yield a more elegant expression and maybe a more efficient implementation, reducing the DNF predicate would obscure the traceability of the logical clauses and interdependence of the behavior rules.

4) Identify State Components and Component Ranges: Continuous components are quantized at integer scale in permissible ranges. For example, system demand is in the range of [0, 1000 GW] and duty cycle is in the range of [0, 100%]. Table VII shows a complete list of the permissible ranges of state components. The resulting HE automation has $2 \times 1001 \times 101 \times 100 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 = 1.294 \times 10^9$ states. The resulting DAP automation has $1001 \times 1001 \times 2 \times 2 \times 11 \times 11 \times 2 \times 2 \times 2 \times 2 = 7.759 \times 10^9$ states. The resulting SEM automaton has $2^{32} \times 2 \times 100 \times 2 \times 1001 \times 2 \times 2 \times 2 \times 2 \times 91 \times 1001 = 2.506 \times 10^{21}$ states. All of these automata are too large; this state explosion is dealt with in the next step.

5) Manage State Space: To manage the number of states, the size of the state machine is reduced by abbreviating the values for some components. Only three values are relevant for system, micro grid and subscriber demand: below threshold, normal and above threshold. Therefore, the domains for these components are collapsed to three values for the HE, DAP and SEM, respectively. This treatment yields a modest HE state machine with $2 \times 3 \times 3 \times 3 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 = 3456$ states, out of which 1008 are identified as safe states and 2448 are unsafe states. Only two values are relevant for networking: whether or not packets forwarded and packets received differ by more than some threshold. Therefore, the domain for this component is collapsed to two values. This treatment yields a modest DAP state machine with $3 \times 3 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 3 = 1728$ states, out of which 255 are identified as safe states and 1473 are unsafe states. Only three values are relevant for rate: below threshold, normal and above threshold. Also, only two values are relevant for usage reporting: current or missing. Therefore, the domains for these components are collapsed to three and two values, respectively. This treatment yields a modest SEM state machine with $2 \times 2 \times 3 \times 2 \times 3 \times 2 \times 2 \times 2 \times 2 \times 3 = 3456$ states, out of which 396 are identified as safe states and 3060 are unsafe states.

E. Collect Compliance Degree Data

BRIDS relies on the use of monitor nodes, e.g., an SEM or a DAP is a monitor node of another SEM. The monitor node knows the state machine of the trustee node assigned to it. The monitor node periodically measures the amount of time the trustee node stays in safe and unsafe states as the trustee node migrates from one state to another triggered by events causing state transitions. A binary grading policy, i.e., assigning a compliance degree of 1 to a safe state and 0 to an unsafe state, is considered. Let c be the compliance degree of a device. The compliance degree c of a device essentially is equal to the proportion of the time the device is in safe states. Let $\mathcal{S}$ be the set of safe states the trustee node traverses over a period of time T. Let t_i be the sojourn time that the trustee node stays in a safe state i, as measured by the monitor node. Then the monitor node collects an instance of c by:

$$c = \frac{\sum\limits_{i \in \mathcal{S}} t_i}{T} \tag{1}$$

If a node stays only in safe states during T, then by (1), its compliance degree c is one. On the other hand, if a node stays only in unsafe states only during T, then its compliance degree c is zero. The monitor node monitors and collects the trustee node's compliance degree history $c_1, c_2, \ldots, c_n$ for n monitoring periods, where n is sufficiently large, based on which it concludes whether or not the trustee node is compromised.

The state machines generated are leveraged to collect compliance degree data of a good and a bad node. With (1), the compliance degree c is essentially equal to the sum of the probabilities of safe states i.e., $c = \sum_{j \in \mathcal{S}} \pi_j$, where π_j is the limiting probability that the node is in state j of the state machine and S is the set of safe states in the state machine. Compliance degree history $c_1, c_2, \ldots, c_n$ of a node is then collected by means of Monte Carlo simulation. That is, given a good (or a bad) node's state machine, start from state 0 and then follow the stochastic process of this node as it goes from one state to another. This is continued until at least one state is reentered sufficiently often (say 100 times). Then π_j is calculated using the ratio of the number of transitions leading to state j to the total number of state transitions. Then one instance of compliance degree is collected. A sufficiently large n test runs was repeated to collect $c_1, c_2, \ldots, c_n$ needed for computing the distribution of the compliance degree of a good or a bad node performing reckless or random attacks.

F. Compliance Degree Distribution

The measurement of compliance degree of a device frequently is not perfect and can be affected by noise and unreliable wireless communication in the WAN, NAN and HAN segments. The compliance degree is modeled by a random variable X with $G(\cdot) = Beta(\alpha, \beta)$ distribution [18], with the value 0 indicating that the output is totally unacceptable (zero compliance) and 1 indicating the output is totally acceptable (perfect compliance), such that $G(a)$, $0 \leq a \leq 1$, is given by

$$G(a) = \int_0^a \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1}(1-x)^{\beta-1}dx \tag{2}$$

and the expected value of X is given by

$$E_B[X] = \int_0^1 x \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1}(1-x)^{\beta-1}dx = \frac{\alpha}{\alpha+\beta} \tag{3}$$

The α and β parameters are to be estimated based on the method of maximum likelihood by using the compliance degree history collected $(c_1, c_2, \ldots, c_n)$ during the system's testing phase. The maximum likelihood estimates of α and β are obtained by numerically solving the following equations:

$$\begin{aligned} \frac{n\frac{\partial\Gamma(\hat{\alpha}+\hat{\beta})}{\partial\hat{\alpha}}}{\Gamma(\hat{\alpha}+\hat{\beta})} - \frac{n\frac{\partial\Gamma(\hat{\alpha})}{\partial\hat{\alpha}}}{\Gamma(\hat{\alpha})} + \sum_{i=1}^{n} \log c_i = 0 \\ \frac{n\frac{\partial\Gamma(\hat{\alpha}+\hat{\beta})}{\partial\hat{\beta}}}{\Gamma(\hat{\alpha}+\hat{\beta})} - \frac{n\frac{\partial\Gamma(\hat{\beta})}{\partial\hat{\beta}}}{\Gamma(\hat{\alpha})} + \sum_{i=1}^{n} \log(1-c_i) = 0 \end{aligned} \tag{4}$$

where

$$\frac{\partial\Gamma(\hat{\alpha}+\hat{\beta})}{\partial\hat{\alpha}} = \int_0^\infty (\log x) x^{\hat{\alpha}+\hat{\beta}-1} e^{-x} dx.$$

A less general, though simpler model, is to consider a single parameter $Beta(\beta)$ distribution with α equal to 1. In this case, the density is $\beta(1-x)^{\beta-1}$ for $0 \leq x \leq 1$ and 0 otherwise. The maximum likelihood estimate of β is

$$\hat{\beta} = \frac{n}{\sum_{i=1}^{n} \log\left(\frac{1}{1-c_i}\right)} \tag{5}$$

The reason the $Beta$ distribution is chosen is that the domain of the $Beta$ distribution can be viewed as a probability, so it can be used to describe the prior distribution over the probability (of a distribution) which models the node compliance degree. By applying Bayesian inference, the $Beta$ distribution then can be used as the posterior distribution of the probability after observing sufficient instances.

G. False Negative and Positive Probabilities

Our intrusion detection technique is characterized by false negative and false positive probabilities, denoted by p_{fn} and p_{fp}, respectively. A false negative occurs when a bad node is missed as a good device, while a false positive occurs when a good node is misdiagnosed as a bad device. While neither is desirable, a false negative is especially impactful to the system's continuity of operation. In this paper, a threshold criterion is considered. That is, if a bad node's compliance degree denoted by X_b with a probability distribution obtained by (2) is higher than a system minimum compliance threshold C_T, then there is a false negative. Suppose that the compliance degree X_b of a bad node is modeled by a $G(\cdot) = Beta(\alpha, \beta)$ distribution. Then the host IDS false negative probability p_{fn} is given by

$$p_{\text{fn}} = \Pr\{X_b > C_T\} = 1 - G(C_T). \tag{6}$$

On the other hand, if a good node's compliance degree denoted by X_g is less than C_T, then there is a false positive. Again suppose that the compliance degree X_g of a good node is modeled by a $G(\cdot) = Beta(\alpha, \beta)$ distribution. Then the host false positive probability p_{fp} is given by

$$p_{\text{fp}} = \Pr\{X_g \leq C_T\} = G(C_T). \tag{7}$$

III. Numerical Data

Numerical data is reported in this section. A sequence of compliance degree values $(c_1, c_2, \ldots, c_n)$ is first collected for a good or bad device based on Monte Carlo simulation. Equation (5) is then applied to compute the β parameter value of $G(\cdot) = Beta(\alpha, \beta)$ for the probability distribution of the compliance degree for a good device or a bad device performing random attacks. p_{fn} and p_{fp} are then calculated by (6) and (7), respectively. The minimum compliance threshold C_T is then adjusted to control p_{fn} and p_{fp} obtainable. With p_{err} a monitor node can misidentify the status the trustee node is in. p_{err} is set to 0.010, 0.015 and 0.020 for HE, DAP and SEM nodes, respectively. This is because 1–2% mis-monitoring due to ambient noise and wireless communication faults in these environments is reasonable. This is based on Lin and Latchman reporting a 0.11–2.04% Power Line Communication packet error rate [15] and Hong *et al.* reporting a 0.02–4% failure rate [11]. The mis-monitoring error probability of an SEM toward another SEM is higher than that of a DAP toward another DAP, or an HE toward another HE because of limited range and capability of an SEM device.

Tables VIII, IX and X show the β values and the resulting p_{fn} and p_{fp} values when C_T is 0.9 (C_T is a design parameter

TABLE VIII
β IN $\mathrm{Beta}(1, \beta)$ AND RESULTING p_{fn} AND p_{fp} VALUES UNDER VARIOUS ATTACK MODELS FOR HE ($C_T = 0.90$)

Attack Type	β	p_{fn}	p_{fp}
Random ($p_a = 1.00$)	99.5	<0.001%	2.30%
Random ($p_a = 0.80$)	4.33	0.0047%	2.30%
Random ($p_a = 0.40$)	1.10	7.99%	2.30%
Random ($p_a = 0.20$)	0.633	23.3%	2.30%
Random ($p_a = 0.10$)	0.449	35.5%	2.30%
Random ($p_a = 0.05$)	0.353	44.3%	2.30%

TABLE IX
β IN $\mathrm{Beta}(1, \beta)$ AND RESULTING p_{fn} AND p_{fp} VALUES UNDER VARIOUS ATTACK MODELS FOR DAP ($C_T = 0.90$)

Attack Type	β	p_{fn}	p_{fp}
Random ($p_a = 1.00$)	49.6	<0.001%	4.59%
Random ($p_a = 0.80$)	4.19	0.0064%	4.59%
Random ($p_a = 0.40$)	1.10	7.89%	4.59%
Random ($p_a = 0.20$)	0.644	22.7%	4.59%
Random ($p_a = 0.10$)	0.464	34.3%	4.59%
Random ($p_a = 0.05$)	0.372	42.5%	4.59%

TABLE X
β IN $\mathrm{Beta}(1, \beta)$ AND RESULTING p_{fn} AND p_{fp} VALUES UNDER VARIOUS ATTACK MODELS FOR SEM ($C_T = 0.90$)

Attack Type	β	p_{fn}	p_{fp}
Random ($p_a = 1.00$)	32.8	<0.001%	6.87%
Random ($p_a = 0.80$)	4.06	0.0086%	6.87%
Random ($p_a = 0.40$)	1.11	7.78%	6.87%
Random ($p_a = 0.20$)	0.656	22.1%	6.87%
Random ($p_a = 0.10$)	0.479	33.2%	6.87%
Random ($p_a = 0.05$)	0.390	40.7%	6.87%

to be fine-tuned to trade high false positives for low false negatives). Because the expected compliance degree following a $Beta(\alpha, \beta)$ distribution is $\alpha/(\alpha + \beta)$ as given by (3), it is seen that β is close to 0 for a good node or a hidden bad node with a low attack probability (e.g., $p_a = 0.05$) since such a node will have the average compliance degree close to 1. On the other hand, β is much larger than 0 for a bad node with a high attack probability (e.g., $p_a = 1$) since such a node will have the average compliance degree much lower than 1.

It is observed that when the random attack probability p_a is high, the attacker can be easily detected as evidenced by a low false negative probability. Especially when $p_a = 1$, a reckless attacker can hardly be missed. On the other hand, as p_a decreases, the attacker becomes more hidden and insidious, and the false negative probability increases. The false positive probability remains the same regardless of the random attack probability because it is not related to the attacker behavior.

By adjusting C_T, the specification-based IDS technique can effectively trade higher false positives for lower false negatives to cope with more sophisticated and hidden random attackers. This is especially desirable for ultra safe and secure applications for which a false negative may have a dire consequence. Fig. 2 shows a *Receiver Operating Characteristic* (ROC) graph of intrusion detection rate (i.e., $1 - p_{\mathrm{fn}}$) versus false positive probability (p_{fp}) obtained as a result of adjusting C_T. In Fig. 2 there are several curves for each node type, one for each random attacker case with a different attack probability p_a. As C_T is increased, the detection rate increases (vertically up on a ROC graph) while the false probability increases (toward the right of

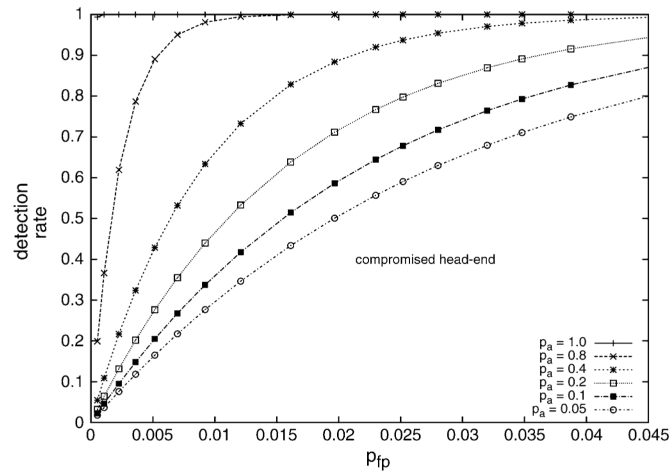

Fig. 2. HE receiver operating characteristic graph.

a ROC graph). It is seen that with the specification-based IDS technique, the detection rate of the node can approach 100% for detecting attackers, that is, an attacker is always detected with probability 1 without false negatives, while bounding the false positive probability to below 0.2% for reckless attackers and below 6% for random attackers.

IV. Comparative Analysis

The performance of BRIDS is compared with contemporary anomaly-based IDSs for HEs, DAPs and SEMs, including CLONALG and AIRS2Parallel [22], [23], LOUD, LOED, LOUD-GLR and LOED-GLR [10]. Zhang *et al.* [23] reported that CLONALG had a false positive rate of 0.7% and a false negative rate of 21.02% and AIRS2Parallel had a false positive rate of 1.3% and a false negative rate of 26.32%. Zhang *et al.* [22] further compared the effectiveness of audit data from three sources: home IDS (HIDS), neighborhood IDS (NIDS) and wide-area IDS (WIDS). These three approaches correspond with the SEM, DAP and HE nodes identified in Fig. 1. Here the authors reported that CLONALG had an accuracy of 99.70% for HEs, 80.10–97.00% for DAPs and 93.90–99.30% for SEMs. They reported that AIRS2Parallel had an accuracy of 91.50% for HEs, 82.10–96.10% for DAPs and 95.10–98.70% for SEMs. The authors provided no p_{fn} or p_{fp} information, but presumably the worst detection accuracy is obtained when p_{fp} is very low. He and Blum [10] investigated LOUD, LOED, LOUD-GLR and LOED-GLR approaches to anomaly-based IDS. They fixed the false positive probability (i.e., p_{fp}) at 0.1% and showed that the detection rate (i.e., $1 - p_{\mathrm{fn}}$) for each approach varies over a wide range based on the parameterization. The LOUD-GLR approach reportedly performs the best with the detection accuracy of $100 - 0.1 - 5 = 94.9\%$.

Tables XI, XII and XIII summarize the comparative performances among contemporary IDSs for HE, DAP and SEM devices, respectively. The performance metric is *detection accuracy* defined as $1 - p_{\mathrm{fp}} - p_{\mathrm{fn}}$. For cases where p_{fn} and p_{fp} are reported [10], [23], the detection accuracy value is shown following the $1 - p_{\mathrm{fp}} - p_{\mathrm{fn}}$ format. For cases where p_{fn} and p_{fp} are not reported [22], the detection accuracy value or a range of detection accuracy values is shown only. For comparison, the

TABLE XI
COMPARISON RESULTS FOR HE

Approach	Detection Accuracy	Device
CLONALG [23]	100-0.7-21.02 = 78.28%	HE
AIRS2Parallel [23]	100-1.3-26.32 = 78.38%	HE
LOUD [10]	100-0.1-9 = 90.90%	HE
LOED [10]	100-0.1-16 = 83.90%	HE
LOUD-GLR [10]	100-0.1-5 = 94.90%	HE
LOED-GLR [10]	100-0.1-9 = 90.90%	HE
CLONALG WIDS [22]	99.70%	HE
AIRS2Parallel WIDS [22]	91.50%	HE
BRIDS ($C_T = 0.50$)	100-0.70-0.00 = 99.30%	HE
BRIDS ($C_T = 0.73$)	100-1.30-0.00 = 98.70%	HE
BRIDS ($C_T = 0.09$)	100-0.10-0.01 = 99.89%	HE

TABLE XII
COMPARISON RESULTS FOR DAP

Approach	Detection Accuracy	Device
CLONALG NIDS [22]	[80.10, 97.00%]	DAP
AIRS2Parallel NIDS [22]	[82.10, 96.10%]	DAP
BRIDS ($C_T = 0.37$)	100-0.70-0.00 = 99.30%	DAP
BRIDS ($C_T = 0.58$)	100-1.30-0.00 = 98.70%	DAP
BRIDS ($C_T = 0.06$)	100-0.10-1.68 = 98.22%	DAP

TABLE XIII
COMPARISON RESULTS FOR SEM

Approach	Detection Accuracy	Device
CLONALG HIDS [22]	[93.90, 99.30%]	SEM
AIRS2Parallel HIDS [22]	[95.10, 98.70%]	SEM
BRIDS ($C_T = 0.29$)	100-0.70-0.00 = 99.30%	SEM
BRIDS ($C_T = 0.47$)	100-1.30-0.00 = 98.70%	SEM
BRIDS ($C_T = 0.05$)	100-0.10-7.82 = 92.08%	SEM

adversary is configured with $p_a = 1$ (reckless attacks). BRIDS performance is shown for $C_T = 0.50$ for HE, $C_T = 0.37$ for DAP and $C_T = 0.29$ for SEM to approximate the CLONALG p_{fp} of 0.7% [23]. BRIDS performance is shown for $C_T = 0.73$ for HE, $C_T = 0.58$ for DAP and $C_T = 0.47$ for SEM to approximate the AIRS2Parallel p_{fp} of 1.3% [23]. BRIDS performance is shown for $C_T = 0.09$ for HE, $C_T = 0.06$ for DAP and $C_T = 0.05$ for SEM to approximate the LOUD, LOED, LOUD-GLR and LOED-GLR p_{fp} of 0.1% [10].

Tables XI, XII and XIII support the claim that by effectively adjusting C_T to trade false positives for low false negatives, BRIDS outperforms existing anomaly-based IDS approaches, especially for HE and DAP devices.

V. CONCLUSIONS

For a modern electrical grid, being able to detect attackers while limiting the false positive probability to protect the continuity of operation is of utmost importance. In this paper, a behavior-rule specification-based IDS technique for intrusion detection of physical devices was proposed. The utility by head-ends, distribution access points/data aggregation points and subscriber energy meters was exemplified. This study also demonstrated that the detection probability approaches one (that is, the attacker can always be caught without false negatives) while bounding the false positive probability to below 0.2% for recklers attackers and below 6% for random attackers (that is, the probability of misidentifying a good node as a bad node can always be bounded to a very low level). Through a comparative analysis, it was demonstrated a behavior-rule specification-based IDS technique outperforms existing anomaly-based IDS approaches for detecting intruders.

Two future research directions extending from this study are (a) investigating and analyzing intrusion response and repair strategies [17]; and (b) implementing behavior rules on applications. Possible intrusion responses include evicting individual compromised nodes, isolating compromised segments (micro grid or larger scope) and adjusting IDS parameters (e.g., T_{IDS}, m and C_T) to increase detection strength. Possible repair strategies are to identify compromised segments and for each one: stop operating, revert all nodes to certified software loads and configurations, rekey/reset passwords and progressively resume operation from the production side of the network towards the subscribers. Possible implementation strategies are to encode the state machine, host IDS software and system IDS software in a high-level language, cross-compile for the targets of interest, deploy and tune the parameterization (e.g., T_{IDS}, m and C_T) based on desired versus actual false negative and positive rates. Another future research direction is to investigate other intrusion detection criteria [1], [4], [5] based on accumulation of deviation from good states in addition to the current binary criterion used in the paper based on a minimum compliance threshold to further improve the detection rate without compromising the false positive probability.

REFERENCES

[1] F. B. Bastani, I. R. Chen, and T. W. Tsao, "Reliability of systems with fuzzy-failure criterion," in *Proc. Ann. Reliab. Maintainab. Symp.*, Anaheim, CA, USA, Jan. 1994, pp. 442–448.

[2] R. Berthier and W. Sanders, "Specification-based intrusion detection for advanced metering infrastructures," in *Proc. IEEE 17th Pacific Rim Int. Symp. Dependable Computing*, Dec. 2011, pp. 184–193.

[3] 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. 6th ACM Symp. Inf., Comput. Commun. Security*, Hong Kong, Mar. 2011, pp. 355–366.

[4] I. R. Chen and F. B. Bastani, "Effect of artificial-intelligence planning-procedures on system reliability," *IEEE Trans. Reliab.*, vol. 40, no. 3, pp. 364–369, 1991.

[5] I. R. Chen, F. B. Bastani, and T. W. Tsao, "On the reliability of AI planning software in real-time applications," *IEEE Trans. Knowledge Data Eng.*, vol. 7, no. 1, pp. 4–13, Jan., 1995.

[6] Y. Chen and B. Luo, "S2a: Secure smart household appliances," in *Proc. 2nd ACM Conf. Data Application Security Privacy*, San Antonio, TX, USA, Feb. 2012, pp. 217–228.

[7] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes, "Using model-based intrusion detection for SCADA networks," in *Proc. SCADA Security Scientific Symp.*, Miami, FL, USA, Jan. 2007, pp. 127–134.

[8] A. da Silva, "Decentralized intrusion detection in wireless sensor networks," in *Proc. 1st ACM Int. Workshop Quality Service Security Wireless Mobile Netw.*, 2005, pp. 16–23.

[9] B. Dutertre, "Formal modeling and analysis of the modbus protocol," *Critical Infrastructure Protection*, pp. 189–204, 2007.

[10] Q. He and R. S. Blum, "Smart grid monitoring for intrusion and fault detection with new locally optimum testing procedures," in *Proc. 2011 IEEE Int. Conf. Acoustics, Speech Signal Process.*, May 2011, pp. 3852–3855.

[11] Y.-F. Hong, Z.-Q. Liu, H.-X. Yin, and J.-H. Zhang, "A new method for smart grid reliability," in *Proc. 2011 Asia-Pacific Power Energy Eng. Conf.*, Mar. 2011, pp. 1–4.

[12] K. Ioannis, T. Dimitriou, and F. Freiling, "Towards intrusion detection in wireless sensor networks," in *Proc. 13th Eur. Wireless Conf.*, 2007.

[13] P. Jokar, H. Nicanfar, and V. Leung, "Specification-based intrusion detection for home area networks in smart grids," in *Proc. 2011 IEEE Int. Conf. Smart Grid Commun.*, Oct. 2011, pp. 208–213.

[14] R. Klump and M. Kwiatkowski, "Distributed ip watchlist generation for intrusion detection in the electrical smart grid," *Critical Infrastructure Protection IV*, vol. 342, pp. 113–126, 2010.
[15] Y.-J. Lin and H. Latchman, "On the effects of maximum transmission unit in power line communication networks," in *Proc. IEEE Int. Symp. Power Line Commun. Its Applications*, Mar. 2007, pp. 511–516.
[16] B. Luitel, G. Venayagamoorthy, and C. Johnson, "Enhanced wide area monitoring system," in *Proc. Innovative Smart Grid Technol.*, Jan. 2010, pp. 1–7.
[17] R. Mitchell and I. R. Chen, "Effect of intrusion detection and response on reliability of cyber physical systems," *IEEE Trans. Reliab.*, vol. 62, no. 1, pp. 199–210, Mar. 2013.
[18] S. M. Ross*, Introduction to Probability Models*, 10th ed. New York, NY, USA: Academic, 2009.
[19] C.-W. Ten, J. Hong, and C.-C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 865–873, Dec. 2011.
[20] X. Wang and P. Yi, "Security framework for wireless communications in smart distribution grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 809–818, Dec. 2011.
[21] Y. Wang, D. Ruan, J. Xu, M. Wen, and L. Deng, "Computational intelligence algorithms analysis for smart grid cyber security," in *Advances in Swarm Intelligence*, Y. Tan, Y. Shi, and K. Tan, Eds., 2010, vol. 6146, Lecture Notes in Computer Science, pp. 77–84.
[22] Y. Zhang, L. Wang, W. Sun, R. Green, and M. Alam, "Artificial immune system based intrusion detection in a distributed hierarchical network architecture of smart grid," in *Proc. IEEE Power Energy Soc. General Meeting*, Detroit, MI, USA, Jul. 2011, pp. 1–8.
[23] Y. Zhang, L. Wang, W. Sun, R. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 796–808, Dec. 2011.

Rob Mitchell received the B.S. and M.S. degrees in computer science from Virginia Polytechnic Institute and State University, Falls Church, VA, USA, in 1997 and 1998, respectively, where he is currently pursuing the Ph.D. degree in the Department of Computer Science.

His research interests include security, mobile computing, sensor networks, embedded systems, and coding and information theory.

Ing-Ray Chen (M'98) received the B.S. degree from the National Taiwan University, Taipei, Taiwan, and the M.S. and Ph.D. degrees in computer science from the University of Houston, Houston, TX, USA.

He is a professor in the Department of Computer Science at Virginia Polytechnic Institute and State University, Falls Church, VA, USA. His research interests include mobile computing, wireless networks, security, intrusion detection, trust management, real-time intelligent systems, and reliability and performance analysis.

Dr. Chen currently serves as an Editor for IEEE COMMUNICATIONS LETTERS, IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, *Wireless Communications and Mobile Computing*, *The Computer Journal*, *Wireless Personal Communications,* and S*ecurity and Communication Networks*. He is a member of ACM.