Hybrid Control Network Intrusion Detection Systems for Automated Power Distribution Systems

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

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

Abstract—In this paper, we describe our novel use of network intrusion detection systems (NIDS) for protecting automated distribution systems (ADS) against certain types of cyber attacks in a new way. The novelty consists of using the hybrid control environment rules and model as the baseline for what is normal and what is an anomaly, tailoring the security policies to the hybrid control environments and the physical constraints of the system. NIDS sensors in our architecture continuously analyze traffic in the communication medium that comes from embedded controllers, checking if the data and commands exchanged conform to the expected structure of the controllers interactions, and evolution of the system’s physical state. Considering its importance in future ADSs, we chose the fault location, isolation and service restoration (FLISR) process as our distribution automation case study for the NIDS deployment. To test our scheme, we emulated the FLISR process using real programmable logic controllers (PLCs) that interact with a simulated physical infrastructure. We used this testbed to examine the capability of our NIDS approach in several attack scenarios. The experimental analysis reveals that our approach is capable of detecting various attacks scenarios including the attacks initiated within the trusted perimeter of the automation network by attackers that have complete knowledge about the communication information exchanged.

Index Terms—Power distribution systems, distribution automation, network security, intrusion detection systems.

I. INTRODUCTION

A. Scope and Goals

Distribution automation refers to a blend of emerging technologies, such as switching technologies, sensor detectors, and communication protocols, that are utilized to control and monitor the operation of a power distribution system in an automated fashion [1]. The vision for automated distribution systems (ADS) is to facilitate the exchange of both electrical energy and information between system operators, customers, and other parties and equipment [2]. One of the promises of ADS, is to allow the remote control and switching of the power distribution topology for protection and to improve reliability. In such an application, the system operator would be able to automatically locate and isolate the faulted distribution component and restore the electrical service to the healthy parts of the distribution system. The process, called fault location, isolation, and service restoration (FLISR), is expected to considerably reduce the outage duration for customers [3].

Since ADS applications provide remote access to the critical distribution system components through communication networks, it is of paramount importance to coordinate their development with that of an appropriate cyber security framework that would prevent attackers from gaining control of circuit breakers and switches. Unfortunately, despite heightened attention to cyber security issues [4]–[6], existing ADS structures were not designed with cyber security in mind. Moreover, a basic challenge ADSs pose is that their various parts use different communication media and protocols, each with different security requirements.

ADSs are a type of cyber-physical system in which various intelligent physical components communicate to each other through specialized industrial control protocols, e.g., Modbus TCP, DNP3, and IEC 61850. Several information technology-based security standards and systems, including firewalls, encryption schemes, authentication mechanisms, and network intrusion detection systems (NIDS), have been advocated and adopted in order to isolate control networks perimeters from external sources [7]–[9]. Firewalls and NIDS are security mechanisms used to continuously monitor network traffic to determine whether a packet should be accepted based on specific rules and sources allowed inside a network perimeter. Encryption is also a basic computer security tool used to maintain confidentiality of communications. Authentication can be also used to ensure that the sources of commands are legitimate. However, while firewalls and IDSs may protect an ADS against “external” network attacks, based on the way, they are used, they would typically fail when an attack is initiated within the protected system perimeter. Moreover, within a network perimeter, even encryption and authentication fail when an attack or simply an erroneous but damaging command is mistakenly issued by an authorized user [10].

The goal of our work is to augment—but not replace—existing solutions with a novel use of a NIDS. While other NIDS-based solutions exist that can look purely for cyber attacks, our solution also monitors physical activity within the perimeter of plant for potentially damaging commands. This allows our solution to provide utility even in the face of certain “insider” threats and erroneous but damaging commands issued by authorized users of the system and network.

B. Prior Work and Contribution

Network intrusion detection systems (NIDS) are common mechanisms used for real-time monitoring and analysis of
network traffic. They are intended to attempt to identify the presence of events that do not comply with security policies. Security policies are typically based on acceptable information exchange protocols and known network participants, but are often agnostic of the application layer.

We call our use of a NIDS for ADSs a hybrid control NIDS (HC-NIDS) as it incorporates the security policy, control environment rules, physical models and constraints that come from the underlying hybrid control system, to set a baseline and discriminate what is normal from what are instead network anomalies that may reflect an attack.

The idea of using the power system physics, e.g., Ohm’s and Kirchhoff’s Laws, to operate, monitor and protect the grid, is at the heart of power system operation and reliability theories. System physics have previously been used for adequacy and security analysis [11], to filter bad measurement values and to reveal the state of the power grid, as exemplified by State Estimation (SE) and Energy Management Systems (EMS) for the bulk power system [12]. A recent prolific line of work on cyber-physical security has also focused on Byzantine attacks in the SE functionality [13]. This work highlighted vulnerabilities of the bad-data detection step of SE in detecting well-constructed data injection attacks that provide physically valid measurements.

Our work is closer to an approach focusing on detecting possible attacks to hybrid systems used for protection and monitoring on the smart grid. Cárdenas, et al. [14], studied vulnerabilities in hybrid controllers in SCADA systems to network attacks. Their control theoretic approach was related to ours but was more generally focused on process control systems rather than focusing more specifically on power distribution. Lin, et al., [15] proposed to run contingency analyses to predict future consequences of control commands on a critical power asset in the context of transmission network applications. While effective, given the nature of transmission networks, it assumes information about other parts of the system are readily available, as they typically are in the transmission network, but not necessarily in ADSs.

Application of intrusion detection in ADSs has been primarily focused on detection of attacks on the Advanced Metering Infrastructure (AMI) for monitoring purposes [16]. This work is conceptually the closest to what we propose, since it uses known rules about the actual AMI process to identify attacks. However, although the solution described does focus on the process, the process focused on is on the cyber level. We believe that an additional layer of insight and protection in ADSs can be provided by monitoring specific physical constraints and also by leveraging sequential pattern information about legitimate, operational hybrid automata information exchange.

ADTs naturally rely on local sensor measurements, and therefore are intrinsically vulnerable to data injection attacks. However, several parameters that specify local limits of operation can be used to validate changes in data values. Furthermore, most message patterns in these control networks are repetitive, since the processes are automated. Careful accounting for the “cyber” and “physical” context of the information exchanged within the automation network can enhance ability of NIDS to detect attacks, since control message exchanges need not only to be consistent with the control protocol, but also with the specific rules, operational procedures and physical limits known based on the abstract hybrid networked automaton model for the ADS environment. The idea can be viewed as an extension of the concept of formal verification to hybrid cyber-physical systems, which includes the explicit verification of rules used in the hybrid control environment as well as the physics of the system as the basis for NIDS rules.

We demonstrate the utility of our approach through a set of threat scenarios against a FLISR system. In particular, we emulate the operation of the FLISR system for a test distribution feeder using real programmable logic controllers (PLCs) that use the Modbus TCP protocol for communication. We develop intrusion detection rules based on the standard network traffic and operation procedures of the FLISR. We then implement the rules as signatures in the language of a popular, robust, and open-source network monitoring framework called Bro [17]. Those signatures explicitly define acceptable actions, events, and information patterns in the context of the ADS system’s physical model. We demonstrate the features and capabilities of our HC-NIDS by implementing several attack scenarios that either aim to harm the system on a different way, or retrieve information about the status of the physical devices.

The rest of the paper is organized as follows: Section II introduces the various components and discusses the “cyber” vulnerabilities of ADSs. The HC-NIDS for ADS applications is presented in Section III. The implementation of the IDS signatures for the FLISR system is presented in Section IV, where we examine the capability of our approach to detect various attack scenarios. Finally, concluding remarks and future work are given in Section V.

II. AUTOMATED DISTRIBUTION SYSTEMS: STRUCTURE AND CYBER VULNERABILITIES

In the following, we briefly introduce the major components and applications of future ADS, and discuss about the cyber vulnerabilities of these systems.

A. Structure of Automated Distribution Systems

1) Physical Components: The notion of power delivery in distribution systems is evolving to cope with the bi-directional flow of power due to a growing amount of distributed energy resources (DERs) installed in distribution systems. DERs refer to distributed generating units (solar, wind, hydro, or biomass power) and energy storage devices (electric vehicles) that are connected to the medium or low voltage distribution feeders. Power grid customers are also becoming flexible energy consumers by responding to time-varying electricity prices. All these changes in energy production and consumption patterns in distribution systems are driving advances with ADSs [18].

Technical and operational challenges that arise for distribution systems include changes in radial feeder power flow, reverse power flow in distribution lines, loss of effective voltage regulation, and over-current protection scheme coordination.
An effective mean for addressing these challenges is the use of bi-directional reclosers, smart sectionalizers, and advanced protection relaying schemes. The bi-directional switching, through vacuum switch technology, can also support distribution circuit reconfiguration much more quickly than existing switching technologies. Moreover, power electronics-based controllers are key technologies for transforming distribution systems from passive loads to active systems that can inject power into the grid [1].

2) Communication, Control, and Monitoring Components: Communication in ADS include point-to-point and multicast sessions, over wide-area network (WAN) topologies that connect protective relays, sensors, switches, and control centers for monitoring, control and protection purposes. The communication media include power line carrier-based communication, fiber optic, radio systems, and wireless communication, the selection of which depends to the application [18].

The communication infrastructures enable advanced ADS monitoring functions, and include fault detection and location, equipment’s health status identification, performance monitoring of protection systems, etc. Advanced smart sensors are the core components of monitoring systems. They collect data that include basic electrical quantities, i.e., voltage and current, and other quantities that monitor the equipment’s status, fault location, user behavior, environmental parameters and the health of the various elements on the distribution system. ADS sensors have embedded intelligence for local data analysis and communication capabilities to provide smart switching [18].

Various industrial control protocols, including Modbus, DNP3, and IEC 61850, are used in ADS networks. Modbus is an application layer protocol based on a request/response messaging model that follows a master-slave architecture in which the master device is responsible of establishing a connection with slave device(s) that communicate over an Ethernet TCP/IP network. A Modbus packet frame includes a Modbus header that specifies the transaction and protocol IDs, the total number of bytes in the packet to follow, and the device unit ID. The packet frame also includes a Protocol Data Unit section, that specifies the type of action to perform using function codes, the starting reference memory address, and the total number of memory addresses requested. A response can be either normal including the requested information, or can be an exception response, describing the type of error occurred.

B. Cyber Vulnerabilities of Automated Distribution Systems

Some concerns were expressed over cyber security weakness and system fragility of power distribution systems [5], [6]. One of the reasons that exposes ADS to cyber attacks is the fact that development of physical reliability methods has been divorced from a systematic cyber-security assessment off and on-line. In addition, the unconstrained integration of large numbers of communication systems that use open and proprietary network protocols can expose ADS to targeted cyber-attacks. The possible attacks on the ADS include:

1) Denial-of-Service (DoS) Attack: Many components of the ADS are sensitive to timing and require real-time communication to ensure secure and optimal operation of system. An attacker could flood a vital communication link with fabricated packets, causing key packets to be dropped, leading to abnormal operation of the system [20].

2) Man-in-the-Middle and Eavesdropping Attacks: The distribution system spans large geographic areas and communication lines may well be physically unprotected in places. PLCs often communicate through unencrypted protocols that can be identified and analyzed by any open source network analysis tool by tapping into the cable in unguarded location. An attacker can modify the sensor values to the controller, potentially causing the controller to give control commands that send the system into an unsafe state [21]. Related to this, eavesdropping attacks may involve passive listeners of network traffic that reveal sensitive information about the status of physical devices [22].

3) Insider Attack: A person that has some combination of authorized access of or access to a particular system, is commonly considered an insider [23]. Not all insiders are inherently malicious but given that they have knowledge and access of a system that others may not have, may have unusually large ability to damage a system, either maliciously or accidentally. For example, insiders could compromise the system by installing malicious software or hardware equipment on systems not easily accessible by others.

Thus, a variety of possible attacks against confidentiality, integrity, and availability of ADS exist, with the most damaging ones being those in which controllers are made to perform actions that put the system in a physically unsafe state.

III. HYBRID CONTROL NETWORK INTRUSION DETECTION SYSTEM FOR ADS

In this section, we present our HC-NIDS solution for ADS applications. In this paper, we focus on NIDS rules for the FLISR system, as it is one of the widely-used applications of ADSs, although we believe that our technique can apply to ADSs more broadly. We first describe the detailed operation of the FLISR system, and then introduce our approach for securing this application against cyber attacks.

A. Fault Location, Isolation and Service Restoration (FLISR)

Permanent failures of any distribution system equipment, including cables and overhead lines, would cause power outage for electricity customers. Traditionally, distribution system operators had limited monitoring and control access on distribution equipment, which made it a difficult and time-consuming process to manually locate the fault, dispatch the maintenance crew, and finally restore the service for customers.

Integration of remotely-controlled sectionalizing switches (SSs) and fault detectors (FDs) along with peer-to-peer communication between the protection devices enable the application of automatic FLISR in ADS. The FLISR function would automatically detect feeder faults, determine the fault location, isolate the faulted section of the feeder, and restore service to healthy portions of the feeder [18]. This automation of the process would considerably reduce the customers’
outage duration and improve the reliability of the distribution system [3]. The typical radial distribution feeder, shown in Fig. 1, is used to exemplify the FLISR process. The feeder consists of four line sections ($L_i$) which are equipped at both sides with $SS$ and $FD$.

The main feeder energizes the four load points ($LP_i$) through a circuit breaker ($CB$). Consider a permanent fault that occurs on line section $L_\alpha$ in Fig. 1. The FLISR process operates as follows:

1. **Fault Location:** The $CB$ of the main feeder detects the fault, operates and de-energizes all the four downstream load points.
2. **Fault Isolation:** Fault detectors $FD_4$ and $FD_5$ report the location of the fault to the master station. Accordingly, an opening command is sent by the master station to sectionalizing switches $SS_4$ and $SS_5$ to isolate the faulted section.
3. **Service Restoration:** The master station sends a closing command to the feeder $CB$; therefore load points $LP_1$ and $LP_2$ are re-energized.

**B. Hybrid Control NIDS (HC-NIDS)**

Our “hybrid control” use of NIDS is designed to perform real-time monitoring and analysis of network traffic and detect actions that do not conform to a set of predefined operational rules and policies. We leverage the Bro Network Monitoring Framework [17] for a variety of reasons but our technique could be implemented in other IDS frameworks as well. We assume that the Modbus TCP protocol is utilized as the communication protocol between the controllers in FLISR, although our approach applies equally well to other protocols such as DNP3, and indeed the Bro IDS that we use also contains a DNP3 parser, in addition to a Modbus parser.

We use Bro to monitor the network traffic of the FLISR system, and is responsible for identifying any actions that are not consistent with the physical operation and network communication rules of the Hybrid Control scheme that describes FLISR’s normal operation and physical constraints. For this reason, as described earlier, we refer to approach as *Hybrid Control NIDS (HC-NIDS)*. The first layer of the HC-NIDS is an event engine which captures the network traffic, detects every single Modbus packet and forwards the packets to analyze within the second layer which is the rules layer. The captured Modbus packets are analyzed to check their consistency to the IDS rules, reflecting the FLISR process and operational physics. If a packet contains a command that would trigger a deviation from the prescribed process, a log entry or alert is triggered. We have developed several IDS rules, as follows, based on network packets of the FLISR:

1. **IP Address:** Any request packet that has an IP address different than the master’s IP address indicates an attempt of attack.
2. **Function code (fc):** Only write to single coils (fc = 5) commands are allowed. Packets that include any other function code are not acceptable.
3. **Packet sequence:** Based on the FLISR process, only the communication pattern shown in Fig. 2 is valid.
4. **Cycle duration:** The time gap between two “write” commands specified in the expected packet sequence (one cycle) has a relatively constant value. Significant deviations from the average cycle duration suggest a possible attack.
5. **Physical constraints:** Data or actions cannot drive the physical system beyond its safety limits. Sensor measurements should be consistent with physical laws.

**IV. Case Studies Using our Approach**

In order to demonstrate the utility of our approach in protecting cyber vulnerabilities of the FLISR system, we implemented different attack scenarios whose main purpose is to either confound the system or retrieve important information about the system’s state. Our primary goal in describing this assessment is to demonstrate that by leveraging knowledge of the system’s expected behavior, our approach can observe a broad range of potential classes of intrusions, in addition to the typical intrusion detection rules that many existing NIDS employ. Attack scenarios in subsection A show cases where a traditional NIDS works well by checking that the communication rules are not violated. The rest of the attack scenarios demonstrate capabilities largely specific to the approach used in the HC-NIDS.

The experimental set-up of our implementation, as shown in Fig. 3, consists of physical devices, PLCs, and the HC-NIDS. We used two Siemens SIMATIC S7-1200 series PLCs, model

---

**Fig. 1.** FLISR operation process

**Fig. 2.** Communication packet sequence of FLISR

---

<table>
<thead>
<tr>
<th>Request #1</th>
<th>Response #1</th>
<th>Request #2</th>
<th>Response #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>fc=5</td>
<td>Address=6</td>
<td>Status to write</td>
<td>Response #1</td>
</tr>
<tr>
<td>Response #1 received</td>
<td>fc=5</td>
<td>Address=6</td>
<td>Status written</td>
</tr>
<tr>
<td>fc=5</td>
<td>Address=1,2,3 or 4</td>
<td>Status to write</td>
<td>Response #2</td>
</tr>
<tr>
<td>Response #2 received</td>
<td>fc=5</td>
<td>Address=1,2,3 or 4</td>
<td>Status written</td>
</tr>
</tbody>
</table>
CPU 1212C AC/DC/RLY, that are configured to emulate the FLISR system’s tasks and communicate through the Modbus TCP protocol. The master controller emulates the FLISR master station and receives as input data the status of the FDs, that are implemented by digital switches. The slave controller in Fig. 3 emulates the actions of circuit breaker and sectionalizing switches. In order to perform the FLISR functions, the slave controller receives queries from the master controller to enable or disable the circuit breaker and sectionalizing switches. The control algorithm of the FLISR is programmed on both controllers using the ladder logic programming language on the SIMATIC STEP 7 Basic software.

As introduced in previous section, Bro IDS [17] is utilized to implement HC-NIDS which is the core component of our implementation. We used Bro’s Turing-complete language to implement IDS rules in terms of policy scripts that define the allowed scope of the FLISR system. The last part of our experimental implementation is a set of scenarios that demonstrate the capability of the HC-NIDS for detecting several types of attacks. For this purpose, we programmed a Modbus Master Simulator in C that acts as the attacker in the FLISR system. We assume that the attacker initiates a connection with the slave controller during the periods when there is not any packet exchange between the two controllers.

A. Intrusion Detection Using Communication Information

1) DoS Attempt: The main purpose of the DoS attack is to make the slave controller unavailable to its intended master controller. Under the assumption mentioned above, the attacker dispatches queries to the slave controller. The HC-NIDS analyzes the network traffic and checks the expected traffic rules, as described in previous section. In this case, the HC-NIDS determines if a non-acceptable IP address commits queries, and produces an alarm that notifies the network administrator about the suspicious attempt.

2) Data Memory Access: The objective of this attack scenario is to probe the status of physical devices to determine if it is possible to take further action, such as causing power outages. We assume the attacker obtains information about the master controller’s IP address and dispatches a “read” command request. The HC-NIDS determines that a “read” command function code is not in the list of acceptable function codes and generates an alarm indicating an attempted illicit action.

B. Intrusion Detection Using Physical Information

1) De-energizing the Distribution Feeder: In this attack, the attacker aims to de-energize the whole distribution feeder by opening the main feeder CB. We assume the attacker retrieves information of the FLISR network configuration, including the controllers’ IP addresses, the memory allocation, and mapping to the physical devices, and the utilized command function codes. However, we assume that the attacker is not aware of the expected packet sequence.

Based on the information obtained from the network traffic, the attacker sends a “write” command request to open the CB. In this case, the malevolent attempt passes the three intrusion detection rules, i.e., controllers’ IP addresses, command function codes and cycle’s time gap. However, the HC-NIDS detects that the initial packet is not followed by an opening command to the SSs, so it is not consistent with the packet sequence in Fig. 2. More specifically, this attack scenario only includes the exchange of one “write” command query that targets the CB, and thus a faulty packet sequence is observed and the HC-NIDS generates an alert indicating that a malfeasance activity observed.

2) Causing Power Outage for Intended Load Points: In this attack, the attacker aims to cause a power outage for certain load points by isolating specific line sections. We assume that the attacker is aware of the controllers’ IP addresses, the utilized command function codes, and the acceptable packet sequence. However, we assume that the attacker is not aware of the cycle’s duration.

The attacker generates an acceptable packet sequence with the master controller’s IP address and the utilized command function codes. First, the attacker dispatches a “write” command request to activate the CB, and then sends a second “write” command request in order to activate specific SSs. The HC-NIDS observes the time gap between the newly issued queries and detects that the packets’ time gap is not consistent with the expected time gap between two packet requests. This observation triggers the HC-NIDS to issue an alert that indicates the occurrence of a possible malevolent action. Figure 4 shows the timing difference between normal network traffic and several simulated attacks. The attack packets constitute larger time gaps which obviously makes them identifiable in comparison to the normal traffic.

C. An Insider Attack Scenario

This attack is similar to the attack that causes power outages for intended load points. However, we now assume that the
attacker has a complete knowledge about the FLISR process and the network that includes the controllers’ IP addresses, the command function codes, the acceptable packet sequence, and the time gaps between packets. Thus, the attacker is able to dispatch queries that are completely consistent with the system’s expected behavior. We assume that just before the master controller initiates a new block of packets, the attacker takes charge of the connection and initiates a block of packets that follow the observed features of the expected network traffic.

Detecting this attack scenario requires more knowledge about the exact state of the distribution feeder. However, since we are only monitoring one communication path, as we have currently implemented it, the HC-NIDS has incomplete information about the physical state, and insufficient knowledge to detect the attack. A goal of our future work is to mitigate this vulnerability with a decentralized network of HC-NIDS in which the controllers are co-designed with security in mind such that sufficient physical information is available to the HC-NIDS in order to identify physical inconsistencies.

V. CONCLUDING REMARKS AND FUTURE WORK

Securing automated distribution systems is of undoubtedly great importance, due to the fact that security could have severe impacts on the stability, performance and economics of these systems. In order to assess the effects of potential threats, and protect ADS in a more efficient way, we believe that it is necessary to utilize important information related to the physical part of the system for intrusion detection. A deep understanding of the whole system state is required, since the complicated interactions between the physical devices and the communication elements can be used to identify, or even prevent potential malevolent attacks. Our paper identifies the importance of including both the information from physical system operation and network traffic rules in the intrusion detection rules. While this work focuses on smart grid ADS applications, the proposed approach could be applied in order augment the security of other smart grid applications, as well as various cyber-physical systems. As a future effort, we plan to include more details in the IDS rules about the normal operation of the studied process that will emerge from information related to the physical part of the system. Moreover, we plan to examine attack scenarios that simultaneously target geographically distributed physical devices.

REFERENCES