Improving SCADA security of a local process with a power grid model

Justyna J. Chromik
University of Twente,
the Netherlands
j.j.chromik@utwente.nl

Anne Remke
University of Twente, the Netherlands
University of Münster, Germany
anne.remke@uni-muenster.de

Boudewijn R. Haverkort
University of Twente,
the Netherlands
b.r.h.m.haverkort@utwente.nl

Security of networks controlling smart grids is an important subject. The shift of the power grid towards a smart grid results in more distributed control functions, while intrusion detection of the control network mostly remains centrally based. Moreover, existing local (host-based) intrusion detection systems do not yet take into account the physical process itself. Therefore, this work proposes a local intrusion detection system, which considers the outcome of control commands on the physical process. Using two scenarios we explain the benefits of extending the current security measures with a local intrusion detection.

SCADA security, IDS, intrusion detection, process-awareness

1. INTRODUCTION

The power grid is controlled by a Supervisory Control and Data Acquisition (SCADA) network, which allows to centrally execute commands in remote locations and to maintain an overview of the physical system. While this worked well in the traditional power grid, smart grids require more decentralised control at medium and low voltage distribution to ensure a stable and balanced operation.

However, introducing remote controlling capabilities also enables new cyber-attacks, as shown in a test environment (Zeller (2011)), as well as in real life (ICS-CERT (2016)). Security of SCADA systems can be improved by intrusion detection systems (IDSes). Most often they are implemented in a central control room, alerting about intrusions in the control network. Analysing the network traffic, they focus on such aspects like, e.g., whitelisting (Barbosa et al. (2013)), and they do not take process-based information into account. We propose a complementing approach, which is locally installed at the field substations and constantly checks the state of the physical process for safety and consistency. The combination of the two, network-based IDS *and* process-based IDS, is expected to improve the state of the art.

There have been few attempts before to use information about the physical process in IDSes. Bigham et al. (2003) analysed the dependencies between power values in different parts of the network,

treating the anomalies from these dependencies as breaches. Kosek (2016) provided a contextual anomaly detection of the systems controlling the photovoltaic panels, using information about current weather conditions to detect undesirable commands. Isozaki et al. (2014) aim to detect whether sensor readings provided to the controller of a transformer have been tampered with to avoid putting the system in the unwanted voltage range. Also, distributed detection of cyber attacks was already addressed using Fault Detection and Isolation (FDI) filters (Shames et al. (2011); Teixeira et al. (2014); Nishino and Ishii (2014)). Although the above references are able to detect and isolate a faulty node, they do not prevent the fault from happening, as we present in this work.

This paper proposes a local and process-based intrusion detection approach and illustrates its benefits on two different attack scenarios. Introducing such an IDS at each local substation is possible since we only need to maintain a model of the substation and the sensors and actuators that are directly accessible from this substation. Using said model, we are able to detect commands which can be harmful to this system and which may not be identified by a central IDS. While the idea of our model-based IDS approach was already illustrated in (Chromik et al. (2016)), the current paper formalises the topology of the system, and adds checks for transformers, fuses, and protective relays. Furthermore, we tailor the approach for the use in local substations and show that the local intrusion detection complements

Figure 1: Basic topology of SCADA network.

any central mechanisms and is able to improve the overall security.

When assuming that the control network has been bypassed, we are able to show how a complementing local and process-based IDS is able to identify commands that potentially put the system into an unsafe state. This is done by precomputing the system state after the execution of the command in a model using Vision and checking the outcome for safety and consistency.

This paper is organised as follows. Section 2 explains the change in the power grid and how it is controlled. In Section 3 we list the cyber-threats to the smart grid and methods for securing SCADA systems. Section 4 introduces the model and the monitoring of the system, and finally in Section 5 we present two scenarios where our approach improved the security of the power grid. We conclude the paper in Section 6.

2. CONTROLLING THE FUTURE POWER GRID

The power grid ensures that the generated power can reach its consumers. Depending on the function, the power grid is divided into several levels: the generation part, the transmission part, the distribution part and customers. This work only considers the distribution of power which operates in medium voltage (MV) and low voltage (LV), and is controlled by the so-called Distribution System Operator (DSO).

The parties controlling the power grid need to ensure power quality regarding supplied voltage, which may vary due to phase shifts, variations in voltage and/or current magnitude, and voltage unbalance (Bollen and Hassan (2011)). Furthermore, they ensure that the delivered power meets certain requirements, e.g., the generated power must equal the power consumed at any time; in Europe the voltage level at the customer side has to be equal to $230V \pm 10\%$

(EN 50160 (2010)); the *mains frequency* has to stay within $50Hz \pm 0.4\%$.

2.1. Increased automation of power distribution

The control of MV and LV works well in traditional one way of transportation, where the power is generated in one part of the grid, and is provided to another part of the grid (and the controlling functions are maintained centrally). However, the shift from centralised large energy production to decentralised small production from Distributed Energy Resources (DER) creates the necessity of more control and flexibility in the MV and LV. The use of renewable resources is one of the principles of (future) smart grids. Some others include self-healing, enabling participation by consumers, protection against physical and cyber-attacks, power quality, adapting all generation and storage options, enabling new products, services and markets, and performance optimisation (IEA (2011)).

Modernisation of the MV and LV substations will allow remote control of the connected devices by means of a control network. Examples of decentral control mechanisms in the distribution grid are: switching power lines for maintenance; voltage regulation using Load Ratio Control Transformers (LRTs) (Isozaki et al. (2014)); or reducing the peak demand with Conservation Voltage Reduction (CVR) (Hasslinger et al. (2016)).

2.2. Controlling the power grid with SCADA

An example of a SCADA network is shown in Figure 1. This control network manages the physical infrastructure using:

sensors, e.g., voltage meters or phasor measurement units (PMUs) measure values of current and voltage in power lines;

controllers, e.g., a logical program, or an operator control the physical infrastructure; and

actuators, e.g., switches apply the changes.

The data from sensors is collected by Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs), or Programmable Logic Controllers (PLCs), and is sent to a Master Terminal Unit (MTU) located in the control network. The information is then processed by the Energy Management System (described below) and displayed on the Human Machine Interface (HMI), which the operating engineer uses to get an overview of the system. Commands to the actuators and sensor readings are exchanged between the control network and RTUs, IEDs and/or PLCs by means of some communication link, which is typically fibre or GPRS. Some systems also have local control loops, which operate autonomously, e.g. protective relays. The control network is also connected to the corporate network of the company, as shown in Figure 1. This connection is a risk factor for SCADA security. Using a wrong configuration, anyone connected to the Internet can potentially connect to the control network and, e.g., take control over an engineer working station.

Since the power distribution are increasingly modernised, more and more remote substations are equipped with PLCs, RTUs and/or IEDs. These devices have sufficient computational power to host and update our proposed IDS.

2.3. Energy Management System

In order to control the power systems and prevent blackouts, the process operators need to have a good real-time overview of the physical system. Therefore, the information gathered via the SCADA network is processed by an Energy Management System (EMS). Using the power system models and data measured by the sensors, the EMS is able to perform State Estimation (SE) of the state that the power system is in (Liu et al. (2011)). Moreover, it optimises, supervises and controls the power transmission and distribution, and with sufficient amount of data it can detect if a sensor is faulty using Bad Data Detection (BDD). Additionally, using SE the EMS performs Contingency Analysis (CA), which predicts the most severe consequences of a system breakdown, given the state the system is in. The functions of EMS and SCADA are partially overlapping: the control and monitoring parts are the same, but EMS also has the analysis and optimisation capabilities (Zambon et al. (2015)).

While the EMS is able to perform all the named functions: SE, BDD and CA, it is still prone to several cyber-attacks. We will discuss this in Section 3. Once such an attack occurs, the system operators may not be aware of the actual state of the physical system.

3. SMART GRID THREATS AND SECURITY

In this section we analyse and compare different attack scenarios on SCADA systems controlling the power grid. In order to understand the importance of the underlying controlled process, we first describe cyber-attacks on the power grid in Section 3.1. Section 3.2 describes several known approaches to intrusion detection.

3.1. Threats to smart grids

The transition to smart grids complicates the management of this system even more. NISTIR *Guidelines for Smart-Grid Cyber Security* point out that the increasing complexity of the power grid can potentially introduce new vulnerabilities, increase exposure to attackers and create new possibilities for unintentional errors (NIST (2010)). There are many threats to the continuous operation of a smart grid; a good overview of these threats is provided by Louis Marinos (2013). Our focus is on attacks with cyber-origin only, and we explain them below.

Damage, Loss of IT assets. We focus on attacks that alter information, such as stealthy attacks, as described by Liu et al. (2011), Teixeira et al. (2010).

Nefarious Activity, Abuse (IT assets). These are attacks with the intention to deliberately interfere with the information systems, e.g., denial of service.

Eavesdropping, Interception, Hijacking. These types of attacks allow for, e.g., undesired communication between the hacker and a device. Examples of these attacks include interception of sensor readings, message replay and man-in-the-middle (MITM) attacks.

Outages, e.g., loss of electricity by disconnecting part of the grid. An outage may be generated by switching or by damaging the devices. An example of the former is the Ukrainian grid hack (ICS-CERT (2016)).

Deliberate physical attacks, which result in physical damage to the system. We only consider attacks which can be initiated using a controlling network, e.g., damaging a generator by connecting and disconnecting it from the grid (Zeller (2011)), overloading power lines by disconnecting crucial power lines, and changing the data set points of devices Zhu et al. (2011).

Not all the parts of the smart grid are susceptible to all types of threats, e.g., it is more difficult to destroy the integrity of the information in a system with many sensors, as this will be detected by the Bad Data Detection. Moreover, since different operators and providers are on different level of implementing smart grid ideas, there may be more or less possibilities to perform an attack.

3.2. Security of SCADA systems

Knowing the importance of the system controlling the power grid, let us discuss the security of this system. The most popular security frameworks list monitoring and intrusion detection systems (IDS) as important measures to improve the security of a cyber-physical system. Intrusion detection is defined as a *security service that monitors and analyses system events for the purpose of finding, and providing real-time (...) warning of, attempts to access system resources in an unauthorised manner* (IEC (2015)). NIST framework (Stouffer et al. (2011)) also lists it as one of the basic security measures, next to antivirus software and file integrity checkers. There are many approaches for intrusion detection. Following the classification tree proposed by Mitchell et al. (2013), we distinguish two dimensions: detection techniques, and audit material.

Detection techniques consist of (i) knowledge-based, (ii) behaviour-based techniques, and (iii) specification-based techniques. Knowledge-based detection techniques analyse the material searching for known patterns of misbehaviour. This approach is quite accurate but does not detect new, unknown attacks. Behaviour-based detection techniques learn the ordinary behaviour of the system based on the material, and look for unusual (anomalous) patterns. This approach is able to detect attacks not known before, but it often classifies harmless unusual patterns as attacks. Finally, the specification-based detection techniques use the pre-defined specification of the system to detect the deviations from this specification. Combinations of the methods also exist, e.g., a behaviour-specification-based methods.

Regarding the **audit material**, there are two approaches for collecting data: (i) host-based, and (ii) network-based. In the host-based approach the analysis is based mostly on the logs of a single device. In the network-based approach the network activities are studied in order to detect breaches.

For our approach it is important to analyse the IDS location: (i) it is centralised, or (ii) localised. The deployment of central IDSes is done, e.g., by implementing a network-based IDS at a central control room. The monitoring of the process in a centralised fashion is also achieved using EMS. However, such central approaches can be compromised, e.g., with MITM attacks. Once the communication between the central control room and the remote substations is compromised, it is crucial to check whether the commands sent to those substations are legitimate. Therefore, implementing an IDS on each RTU, which checks for physical

violations, as we propose, does improve the safety of the overall system.

4. LOCAL MONITORING OF THE SYSTEM STATE

In order to understand how the physical system evolves, we need to formally define the system, its state and the approach taken for the monitoring. Therefore, in Section 4.1 we define the formal description of the system, its state and events. Section 4.2 describes the system monitoring and algorithm outline which will be used to detect the risky states.

4.1. Formal system description

The part of the power distribution system Ω is described as a tuple $\Omega = (\mathcal{P}, \mathcal{B}, \mathcal{L}, \mathcal{S}, \mathcal{M}, \mathcal{T}, \mathcal{R}, \mathcal{F})$, where $\mathcal{P} = \mathcal{P}^G \cup \mathcal{P}^L$ is a set of power sources ($\mathcal{P}^G$) and loads ($\mathcal{P}^L$), $\mathcal{B}$ is a set of buses, $\mathcal{L}$ is a set of power lines, $\mathcal{S}$ is a set of switches, $\mathcal{M}$ is a set of sensors, $\mathcal{T}$ is a set of transformers, $\mathcal{R}$ is a set of protective relays, and $\mathcal{F}$ is a set of fuses. Note that as compared to the work presented before (Chromik et al. (2016)), we extend the system with transformers, protective relays and fuses.

Even though the formal system description we present is general enough to capture a large part of the power grid, in the following we use smaller models that only represent single substations. In power distribution, remote substations are often controlled by just a single RTU, therefore such a RTU has direct access to information about the measurements of the connected power lines, as well as the switches it controls. Depending on the scenario, not all of the elements which are part of Ω , will be a part of the local system, as e.g., not every substation contains a transformer.

4.1.1. System elements

Power lines labelled l_i for $i \in \{1, \dots, |\mathcal{L}|\}$ are defined as follows: $\mathcal{L} \subseteq (((\mathcal{P} \times \mathcal{B}) \cup (\mathcal{T} \times \mathcal{B}) \cup (\mathcal{B} \times \mathcal{B}) \cup (\mathcal{B} \times \mathcal{T}) \cup (\mathcal{B} \times \mathcal{P})), \mathbb{N})$. Buses are labelled b_j for $j \in \{1, \dots, |\mathcal{B}|\}$. Physical characteristics of a power line impose a maximum current of the power line $l_i \cdot I_{max}$. Exceeding this maximum value may damage the power line, e.g., wearing it off much faster. The maximum current capacity is written as a vector $L \cdot I_{max} = \{l_1 \cdot I_{max}, l_2 \cdot I_{max}, \dots, l_{|\mathcal{L}|} \cdot I_{max}\}$ of size $|\mathcal{L}|$. Note that there are special types of power lines, so called feeders. They are usually of much higher current capacity and they are connecting main distribution stations. In our model we consider them as power lines. Also, a single line may consist of multiple connected lines. This may happen, e.g., when a part of a power line is damaged or worn out, or when the line is extended. In such case we will

consider the minimal I_{max} value among the parts of the line.

Each power line can be connected to or disconnected from the bus by means of a switch. We denote the switch as x_k , where $k \in \{1, \dots, |\mathcal{S}|\}$. We denote the state of switch x_k as $x_k.st \in \{0, 1\}$, representing an open (disconnected) and closed (connected) switch, respectively. The vector X collects the states of all the switches and is of size $|\mathcal{S}|$. A simpler version of a switch is a fuse, which melts when an overcurrent occurs. It is not possible to turn the fuse back on, but it is only possible to replace it. We denote the fuse as f_k , where $k \in \{1, \dots, |\mathcal{F}|\}$. We denote the state of fuse f_k as $f_k.st \in \{0, 1\}$. The vector Y collects the states of all the fuses and is of size $|\mathcal{F}|$.

Protective relays are mechanical or digital controllers, which control a switch they are connected to. In case the current measured on the line exceeds some pre-defined value I_{max} , then the switch will be opened, disconnecting the line with over-current. They are denoted as R_i for $i \in \{1, \dots, |\mathcal{R}|\}$, and have to have a switch assigned, i.e., for switch m and relay n , $R_n.x = x_m$.

Next to the switches each power line has meters m (sensors) within the substation where the bus is located.. The sensor m_i measures usually at least the current in the line $m_i.i$, and the voltage between the line and the ground $m_i.v$. The description of the readings from one sensor are written as a pair of the current and voltage readings: $(m_i.i, m_i.v)$.

Transformers connect the parts of a power system operating at different voltage. A transformer T_i for $i \in \{1, \dots, |\mathcal{T}|\}$ has the following properties: transformation rate r , which defines the voltage ratio (e.g., the ratio 1000:1 transforms voltage from 400 kV to 400 V), and the transformer tap position p . The position of the tap has to be chosen in such way that the secondary voltage, i.e., the voltage delivered to the customer, has to be equal 230 V. The measurements are not taken directly on the windings of the transformer. However, measurements taken on the incoming and outgoing lines are an accurate approximation.

The power flows from elements with higher energy to the ones with lower energy, e.g., from a generator to a load. Knowing the power on each bus, we also know which lines are *incoming* to and *outgoing* from the bus. Let $\mathcal{B}_j.in$ denote the subset of lines incoming to the j th bus, and $\mathcal{B}_j.out$ the subset of lines outgoing from the j th bus. Note, that in smart grids there may be customers (houses) that produce electricity using, e.g., solar panels and are able to become a source of electricity. In that case

they can be treated as a source, instead of a load. The amount of power produced at source G_i is denoted $G_i.pv$ and the amount of power consumed at load L_i is denoted $L_i.pv$, respectively. For now we consider constant power loads and sources. Vector P is of size $|\mathcal{P}|$ and collects the current values for all loads and sources. Note that loads are presented as negative values to distinguish them from (positive) source values.

4.1.2. Topology

The way the elements of the system are connected forms a topology. Describing all the elements with the parameters as described in Table 1 explain the topology of the exemplar system depicted in Figure 2. For example, by $l_6 = (b_2, L_1)$ we mean that line 6 is connecting bus 2 with load 1, while by $x_{12} = (l_9, b_2.x)$ we denote that switch 12 is a switch on line 9, on the side of bus 2. In this paper we will use a scheme to depict the topology of (the part of) the system. Note that for clarity of the Figure 2 not all the elements are named.

4.1.3. System state

Let us now formalise the description of a state in the system. The state refers to the values which can change in the system over time. The system state can be described by five vectors indicating: (i) the states of the switches, (ii) the state of the fuses, (iii) the sensor readings, (iv) power consumption and production, and (v) position of the transformer taps.

Firstly, we denote the state of all switches in the system as a vector $X = [x_1.st, x_2.st, \dots, x_{|\mathcal{S}|}.st]$ which is of size $|\mathcal{S}|$. Secondly, we denote the state of all fuses in the system as a vector $Y = [f_1.st, f_2.st, \dots, f_{|\mathcal{F}|}.st]$, which is of size $|\mathcal{F}|$. Thirdly, the readings from one sensor can be written as a pair of the measured current and voltage: $(l_i.m.i, l_i.m.v)$. Vector SR collects those pairs for all sensors: $SR = [(l_1.m.i, l_1.m.v), \dots, (l_{|M|}.m.i, l_{|M|}.m.v)]$, and is of size $|M|$. Next, the vector describing the loads and sources of power is denoted as $P = [G_1.pv, \dots, G_{|PG|}.pv, -L_1.pv, \dots, -L_{|PL|}.pv]$ for $|PG|$ sources and $|PL|$ loads. Finally, we denote the set of positions of the transformer tap as a vector $Z = [T_1.p, T_2.p, \dots, T_{|\mathcal{T}|}.p]$, which is of size $|\mathcal{T}|$.

Now, the system state T can be written as a tuple that consists of the above five vectors: $T = (X, Y, SR, P, Z)$.

4.1.4. Events

The system state can change upon receiving any new information, e.g., information from the sensors with different voltage readings result in an updated state. Different power values of the sources or loads also update the state. Moreover, a

Table 1: Detailed description of the elements of the system (example)

Symbol	Element	Property	Scenario Fig. 2 and 4	Controllable?
Power sources and loads	Name Position Power value	$G_1; L_1$ $G_1.pos = l_1$ $G_1.pv$
Buses	Name Set of incoming lines Set of outgoing lines	b_1 $B_3.in = \{l_8\}$ $B_3.out = \{l_9, l_{15}\}$
Transformers	Name Transformer rate Tap switch position	T_1 $T_1.r$ $T_1.p$	yes
Power lines	Name Maximum current Meter (side of b_2) (side of b_4) Set of meters on line l_3 Switch (side of b_2) (side of b_4) Set of switches on line l_3 Fuse (side of b_5) Set of fuses on line l_{51}	$l_6 = (b_2, b_4)$ $l_6.I_{max}$ $l_6.b_2.m = m_8$ $l_6.b_4.m = m_9$ $\mathcal{L}_6.m = \{m_8, m_9\}$ $l_6.b_2.x = x_8$ $l_6.b_4.x = x_9$ $\mathcal{L}_6.x = \{x_8, x_9\}$ $l_{51}.b_5.f$ $\mathcal{L}_{51}.f = \{f_5\}$
Meters	Name Measured current Measured voltage	$m_8 = l_6.b_2.m$ $l_6.b_2.m.i$ $l_6.b_2.m.v$
Switches	Name State of the switch	$x_9 = l_6.b_4.x$ $l_6.b_4.x.st$	yes
Fuses	Name State of the fuse	$f_5 = l_{51}.b_5.f$ $l_{51}.b_5.f.st$
Protective relays (circuit breakers)	Name Cutting current Controlled switch	$R_9 = l_6.b_4.x$ $R_9.I_{max}$ $R_9.x = x_9$	sometimes

Figure 2: A part of the distribution grid.

command to open or close any of the switches, or changing the tap switch position brings the system to another state. Since we assume constant power sources and loads, let us, for now, only consider two event types: (i) readings, and (ii) commands. Readings update the state to a new state $T' = (X', Y', SR', P', Z')$, whereas a command will result in a new state T' with an updated X' , or/and new vector Z' .

4.1.5. Requirements and restrictions

A reliable and safe operation of a power distribution system can be ensured by satisfying a couple of safety requirements ($\mathcal{R}$) given the physical restrictions ($\mathcal{P}$). The safety requirements need to be taken into account when designing and controlling the system, since any violation of these requirements

may lead to damage in the system. In our work we will consider the following **requirements**:

$\mathcal{R}_1$. The voltage on all lines stays between the boundaries $230V \pm 10\%$, i.e. $\forall l_i \in L (\forall m_j \in \mathcal{L}_i.m (l_i.m_j.v \in [207; 253]))$ in the low voltage area. This follows from the power distribution requirements CENELEC (1988).

$\mathcal{R}_2$. The current in a power line does not exceed the maximum allowed current in that power line, i.e. $\forall l_i \in L (\forall m_j \in \mathcal{L}_i.m (l_i.m_j.i \leq l_i.I_{max}))$. This is defined by the cable producer.

$\mathcal{R}_3$. The power produced by the sources equals the power consumed by loads, i.e. $\sum_{G_i \in PG} G_i.pv = \sum_{L_i \in PL} L_i.pv$. This restriction ensures the grid stability.

$\mathcal{R}_4$. If the current in the power line exceeds the value of the cut-off current of a protective relay, then the switch of this protective relay opens, i.e. $\forall l_i \in L \forall R_j \in \mathcal{R} : R_j.x \in \mathcal{L}_i.x (\forall m_k \in \mathcal{L}_i.m (m_k.i > R_j.I_{max} \Rightarrow R_j.x.st = 0))$.

Moreover, several **physical laws** exist that describe the relationship between different entities of the power grid:

$\mathcal{P}_1$. The sum of current ingoing to a bus must be equal to the sum outgoing from a bus (Kirchoff's current law), $\forall b_i \in B. \left(\sum_{l_j \in B_i.in} l_j.b_i.m.i = \sum_{l_k \in B_i.out} l_k.b_i.m.i \right)$.

$\mathcal{P}_2$. If a switch on a line is open, the values of current and voltage on this line have to be zero: $\forall l_i \in L (\forall x_j \in \mathcal{L}_i.x ((x_j.st = 0) \Rightarrow (\forall m_k \in \mathcal{L}_i.m ((m_k.i = 0) \wedge (m_k.v = 0)))))$.

$\mathcal{P}_3$. Assuming there is no power loss on the lines, the value of current and voltage on the beginning of the line must be equal to the value of the current and voltage at the end of the line, $\forall l_i \in L (\forall m_l, m_k \in \mathcal{L}_i.m (m_l.i = m_k.i) \wedge (m_l.v = m_k.v))$.

$\mathcal{P}_4$. The electric power is equal to voltage times the current in the line $P = V \cdot I$, e.g. $G_1.val = G_1.pos.G_1.m.i \cdot G_1.pos.G_1.m.v$.

$\mathcal{P}_5$. Assuming no losses, the transformer changes the voltage and current value with the ratio r , i.e. $\forall T_i \in \mathcal{T}, m_x, m_y : m_x = l_x.T_i.m \wedge m_y = l_y.T_i.m (T_i.r = m_x.v/m_y.v = m_y.i/m_x.i)$ for m_x belonging to higher voltage area than m_y .

$\mathcal{P}_6$. Every transformer has a function $t(p)$ assigned that defines the transformation rate r depending on the position of the tap switch p , i.e. $\forall T_i \in \mathcal{T} : T_i.r = t(T_i.p)$.

Note that the intrinsic difference between requirements and physical constraints is that requirements are a result of regulations, hence they can be violated, whereas the physical constraints represent physical laws which always have to hold.

4.2. Local monitoring

Monitoring the system state locally at each substation allows to (i) validate whether the system evolves consistently, and (ii) evaluate whether the execution of a command coming from the control room will lead to a safe system state in advance. It is done by checking the requirements $\mathcal{R}_1 - \mathcal{R}_4$ and the physical constraints $\mathcal{P}_1 - \mathcal{P}_6$. The execution of a command is considered to be unsafe if it leads to a system state that violates one of the requirements $\mathcal{R}_1 - \mathcal{R}_4$. On the other hand, if one of the physical

constraints $\mathcal{P}_1 - \mathcal{P}_6$ is violated, this indicates that the information that is available on the system state must be incorrect.

4.2.1. Outline of the algorithm

In Section 4.1.3 we defined the system state as a tuple $T = (X, Y, SR, P, Z)$. Let us distinguish between two system state views maintained by the local IDS: (i) T_O , which is the perceived system state, that the IDS sees by only analysing the sensor readings; and (ii) T_C , which is the Calculated system state obtained using the physical laws of the system. Note that in an ideal world the two system states, T_C and T_O , are the same (within some error margin). The algorithm explaining this process is described in more detail in Chromik et al. (2016), and will be briefly commented on below.

New readings mean that we have reached an entirely new system state $T'_O = (X', Y', SR', P', Z')$, which could be unsafe and/or inconsistent. Therefore, two checks need to be performed: (i) the safety check, which is done by verifying the applicable restrictions: $\mathcal{R}_1 - \mathcal{R}_4$, and (ii) the consistency check, which verifies the physical constraints: $\mathcal{P}_1 - \mathcal{P}_6$. Note that depending on the local scenario, not all of the restrictions and constraints are used. For example, an IDS operating in the medium voltage, does not have to take the voltage restriction $\mathcal{R}_1$ into account.

When receiving a new command, i.e., a new vector X' or Z' , this command is first "executed" in the model - based on knowledge of the current state T_C . If the predicted new state T'_C is safe, the command is executed on the actual system. Otherwise, if the predicted state is unsafe, the command is not executed and a proper alert is sent to the operator, possibly via a different communication channel.

The algorithm also compares the current state of the system T_O , as viewed by the local IDS, to the previously calculated system state T_C . If these two states are not the same (with an error margin of ϵ), this has to be reported to the operator (at the central location), since it indicates a potentially dangerous situation.

5. LOCAL IDS SCENARIOS

In this section we present two scenarios, in which we show that the local IDS improves the security of the system. Section 5.1 shows an attack scenario involving switching, and Section 5.2 shows an attack scenario involving a tap changer on a transformer.

Figure 2 shows part of a distribution network of a small town in the Netherlands, which is controlled by a SCADA network. Most of the symbols in that figure are introduced in Table 1, while some shorthand

Table 2: Switching attack scenario

Action	T_{EMS}	$T_{C_{b_2}}, T_{O_{b_2}}$	$T_{C_{b_3}}, T_{O_{b_3}}$
The hacker gains control over communication channel between SCADA server and RTUs			
The hacker sends false information to EMS: replaying the data from the past	EMS relies on false information	n/a	n/a
The hacker sends a command to RTU on bus b_2 to open line 6	command bypassed EMS; EMS relies on false information	local IDS computes $T_{C_{b_2}}$ and does not see any violation. Command is executed by RTU on bus b_2	the value of the current is increasing on all the connected lines
The hacker sends a command to RTU on bus b_2 to open line 7	command bypassed EMS; EMS relies on false information	local IDS computes $T_{C_{b_2}}$ and does not see any violation. Command is executed by RTU on bus b_2	the value of the current is increasing on all the connected lines
System operator (or hacker) sends a command to RTU on bus b_3 to open switch x_{13} for some maintenance	command is allowed by EMS, because based on old information it cannot detect a violation	n/a	local IDS computes the resulting $T_{C_{b_3}}$ and detects violation. Command is discarded and an alert is sent to the operator (or hacker...).

notations are translated into known symbols in boxes A and B.

We use the power network analysis tool Vision¹ to solve the power flow equations, which determine the distribution of current in the system of a defined topology. With each new command we need to recompute that distribution. This way we obtain the sensor readings in each state of the system in Figure 2.

5.1. Switching scenario

The first scenario focuses on bus b_3 . We assume that the corresponding RTU is equipped with an IDS device, which runs the local monitoring algorithm explained in Section 4.2, which monitors the power lines and controls the switches on these power lines. Note that the switches have additional protection mechanisms, which are activated when an overcurrent occurs. Figure 3 shows the part of the system which the local IDS monitors and controls.

To show how our approach is complementing to existing central approaches, such as the EMS, we show how the system evolves locally and report on both the local and the central view. The central view as displayed on the HMI of the EMS is denoted T_{EMS} . The state of the system that is observed locally by the IDS at the RTU is called T_O , and T_C indicates the state calculated by the local IDS. Table 2, explains the attack scenario in more detail and summarises the resulting view on the system as seen by the EMS, IDS on b_2 , and IDS on b_3 .

We assume that the EMS is corrupted and shows inaccurate data on the screen of the control

¹Accessed via http://www.phasetopphase.nl/nl_products/vision_network_analysis.html

Figure 3: Scenario 1 - switching a power line off.

engineer, and both power lines between b_2 and b_4 are open. This means that all the power needed at bus b_4 has to be transported through bus b_3 . However, this information is not shown on the EMS. The operator decides to open switch x_{13} . Knowing the capacity of power lines (as indicated in Figure 3), and the transported power (listed in Table 3), this RTU can decide whether this action is safe or not. The column “Situation 1” in Table 3 explains the current situation of the system. The column “Situation 2” shows the values calculated by the system. We can see that the command is going to cause overcurrent in line l_9 , since $l_9.I_{max} = 157.5 < 202 = m_{12}.i$, and may wear power line off faster. This risky command should be reported to the SCADA control room, and can

Table 3: Sensor readings in scenario 1

Situation 1	Situation 2
$x_{11}.st = 1$	$x_{11}.st = 1$
$x_{12}.st = 1$	$x_{12}.st = 1$
$x_{13}.st = 1$	$x_{13}.st = 0$
$m_{11}.i = 203$	$m_{11}.i = 201$
$m_{11}.v = 10.606$	$m_{11}.v = 10.607$
$m_{12}.i = 60$	$m_{12}.i = 202$
$m_{12}.v = 10.606$	$m_{12}.v = 10.607$
$m_{13}.i = 144$	$m_{13}.i = 0$
$m_{13}.v = 10.606$	$m_{13}.v = 0$

line l_9 overload

Table 4: Sensor readings in scenario 2

Situation 1	Situation 2
$m_{13}.i = 32$	$m_{13}.i = 32$
$m_{13}.v = 11.032$	$m_{13}.v = 11.032$
$m_{14}.i = 19$	$m_{14}.i = 19$
$m_{14}.v = 11.032$	$m_{14}.v = 11.032$
$m_{15}.i = 13$	$m_{15}.i = 13$
$m_{15}.v = 11.032$	$m_{15}.v = 11.032$
$m_{16}.v = 0.244$	$m_{16}.v = 0.256$
$T_5.p = 0$	$T_5.p = -2$
$T_5.r = 26.14$	$T_5.r = 24.9$

low voltage
value violation
(transformer
properties)

Figure 4: Scenario 2 - controlling a tap switch.

be, e.g., rejected. Note that for this simple analysis the IDS at bus b_3 did not need the information about the lines that are not connected to it. The safety mechanisms used in the switches analysed in this scenario are activated only with higher current suggesting a short circuit, e.g., above 400 A.

Moreover, Table 2 shows that the first two commands sent by the hacker have been executed, because the IDS on bus b_2 could not detect an unsafe state.

5.2. Tap switch scenario

In this scenario, the local IDS is monitoring the messages sent to and from the RTU on bus b_5 and it involves a tap switch of the transformer T_5 . Tap switches in low voltage used to be manually set to some position, because of the predictable voltage drops. With the renewable energy sources, such as photovoltaic panels, this is no longer so predictable. Therefore, more transformers are equipped with tap switches, which are adjusting the settings automatically and locally, (Isozaki et al. (2014)). Often it is also possible to overwrite this setting by a command sent from the central control room. The said scenario is presented in Figure 4.

We assume that the hacker takes control over the EMS, like in previous scenario. He then sends a command to switch the tap setting of the transformer $T_5.p$ from 0 to -2. This results in an increase of the secondary voltage from 244 V to 256 V, as indicated in Table 4. That value is outside of the required range, therefore posing a risk to all connected devices in that neighbourhood. The local IDS rejects such command coming from the central control room and raises an alert at the control room.

6. CONCLUSIONS AND FUTURE WORK

The security of smart grids and their control networks is of a utmost importance. While the body of work on this subject is constantly increasing, still many attacks remain undetected. Hence, this paper proposes a complementing system, that locally uses information about the physical process, that is controlled by a single RTU, e.g., at a substation, to detect undesirable commands. We showed that once the control network is exploited, locally monitoring the system state helps to detect commands which could bring the system to an unsafe state. Together with a network IDS, this complementing system is expected to improve the overall system security.

The current paper extends our previous work on a model-based IDS one with an analysis that can be performed locally by IDSes in field substations, using just the measurements of elements connected to it. We presented two scenarios, where threats which are not visible to the centrally based monitoring system can be avoided locally.

Future work will extend the presented approach by including checks on the number and importance of connected power lines, as provided from contingency analysis. Additionally, we will investigate whether the model used by the local IDS could be extended with information from neighbouring RTUs. We intend to test our method using co-simulation of the power grid and the communication network. We can then better estimate the allowed tolerance between system state T_C and observed system state T_O . We also aim to analyse other scenarios,

such as the control of the inverters for, e.g., PV generation.

ACKNOWLEDGMENTS

This research has been conducted as part of the MOSES project (More secure SCADA through self-awareness) funded by NWO.

REFERENCES

- Barbosa, R. R. R. et al. (2013) Flow whitelisting in scada networks. *International journal of critical infrastructure protection*, 6(3), 150–158.
- Bigham, J. et al. (2003) Safeguarding SCADA systems with anomaly detection. In: *Computer Network Security*. Springer, 171–182.
- Bollen, M. H. and F. Hassan. (2011). *Integration of distributed generation in the power system*, 80. John Wiley & Sons.
- CENELEC. (1988) Harmonisation Document: Nominal voltage for low voltage public electricity supply systems. HD 472 S1.
- Chromik, J. et al. (2016) What's under the hood? Improving SCADA security with process awareness. In: *Joint Workshop on Cyber-Physical Security and Resilience in SmartGrids (CPSR-SG2016)*.
- EN 50160. (2010) NEN-EN 50160:2010, Voltage characteristics of electricity supplied by public distribution networks.
- Hasslinger, G. et al. (2016) SGsim: Co-simulation Framework for ICT-Enabled Power Distribution Grids. In: *Measurement, Modelling and Evaluation of Dependable Computer and Communication Systems*, 9629. 60–76.
- ICS-CERT. (2016, 25, Feb.) Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure. Available from <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01>
- IEA. (2011) Technology Roadmap: Smart Grids. International Energy Agency. Available from https://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf
- IEC. (2015) International Electrotechnical Commission (IEC). IEC 62443 Industrial communication networks - Network and system security.
- Isozaki, Y. et al. (2014). On detection of cyber attacks against voltage control in distribution power grids. In: *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, 842–847.
- Kosek, A. M. (2016) Contextual anomaly detection for cyber-physical security in Smart Grids based on an artificial neural network model. In: *Joint Workshop on Cyber-Physical Security and Resilience in SmartGrids (CPSR-SG2016)*.
- Liu, Y. et al. (2011) False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC)*, 14(1), 13.
- Louis Marinou. (2013) European Union Agency for Network and Information Security (ENISA): Smart Grid Threat Landscape and Good Practice Guide.
- Mitchell, R. et al. (2013) Effect of intrusion detection and response on reliability of cyber physical systems. *Reliability, IEEE Transactions on*, 62(1), 199–210.
- Nishino, H. and H. Ishii. (2014) Distributed detection of cyber attacks and faults for power systems. *IFAC Proceedings Volumes*, 47(3), 11932–11937.
- NIST. (2010) Guidelines for Smart Grid Cyber Security. Technical Report 7628, National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA.
- Shames, I. et al. (2011) Distributed fault detection for interconnected second-order systems. *Automatica*, 47(12), 2757–2764.
- Stouffer, K. et al. (2011). NIST guide to industrial control systems (ICS) Security, Second Public Draft. *NIST Special Publication*, 800-82.
- Teixeira, A. et al. (2010) A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator. *arXiv preprint arXiv:1011.1828*.
- Teixeira, A. et al. (2014) Distributed fault detection and isolation resilient to network model uncertainties. *IEEE transactions on cybernetics*, 44(11), 2024–2037.
- Zambon, E. et al. (2015, Jan.) D2.3 Reference Taxonomy on Industrial Control Systems Networks for Utilities. Technical report. Technical Report, PREEMPTIVE.
- Zeller, M. (2011) Myth or reality – does the aurora vulnerability pose a risk to my generator? In: *Protective Relay Engineers, 2011 64th Annual Conference for*, 130–136.
- Zhu, B. et al. (2011). A taxonomy of cyber attacks on SCADA systems. In: *Internet of things (iThings/CPSCoM), 2011 international conference on and 4th international conference on cyber, physical and social computing*, 380–388.