Towards an Implementation of Data Analytics for Smart Grid Security

Jacobo Blanco*, Silvio La Porta*, Niamh O'Mahony*, Rohan Chabukswar†,
Alie El-Din Mady† and Menouer Boubekeur†
*EMC Research Europe, Cork Ireland
Email: {jacobo.blanco,silvio.laporta,niamh.omahony}@emc.com
†United Technologies Research Center, Cork Ireland
Email: {chabukr,madyaa,boubekm}@utrc.utc.com

***Abstract*—Given the recent increase in frequency, sophistication and success of cyber-attacks against critical IT infrastructure, such as the Smart Grid, the urgent need for advanced cyber-security solutions is clearly evident. This paper presents a security information analytics (SIA) framework, using various data analytics methods to detect anomalies in metered data, that may indicate attacks. The implementation of the SIA tool has been applied to a live micro-grid test-bed for the modeling of normal behaviour and for performance analysis. Furthermore, the framework is scalable, allowing additional analysis tools and resilient control solutions to be incorporated, further enhancing the reliability of the system.**

Keywords–Cyber-physical systems; Intrusion detection; Cyber-security

I. INTRODUCTION

Critical infrastructures have, traditionally, been operated as stand-alone systems, with dedicated communication networks, thus protecting them from the outside world. However, advances in Cyber-Physical Systems (CPS), like the smart grid, expose new vulnerabilities, which can be exploited by cyber-criminals intent on carrying out malicious attacks [1], [2]. Recent cyber-attacks on energy utilities demonstrate that cyber-criminals are increasingly targeting critical infrastructures and learning how interact with and use such systems.

For example, on December 23, 2015, hackers deployed malware into the systems of multiple regional power distribution companies in Ukraine, causing an outage that left around 700,000 customers without electricity. The attackers used BlackEnergy along with a destructive component called KillDisk to disrupt machines, thus increasing the time required to restore normal operational mode and remove evidence of an attack [3]. Whilst the first version of BlackEnergy was only a common trojan, able to execute different DDoS attacks[4], it was later reconfigured and extended by incorporating modules to target industrial control systems (ICS). The Sandworm Team, to whom the Ukrainian attack has been attributed [5], are known to have carried out previous attacks, which were reported to not only involve classic strategic espionage, but also to target SCADA systems [6], leveraging a supplementary module in BlackEnergy that scans an IP block for open ports used by SCADA control systems. Furthermore, recently surfaced malware, such as Havex, exhibits the capability to target control systems. Havex was originally used between 2011 and 2013 during the 'DragonFly' campaign [7] that targeted energy, gas and oil companies, in which one of the infection vectors used was the water hole technique – compromising SCADA software companies' websites by repacking malware with the legitimate software.

An important feature of the malware described above is its ability to capture screenshots and record operators' activities in the compromised machines, thus, remedying the attackers' lack of expert knowledge about the ICS. With knowledge of the system model, an attacker may successfully achieve an attack which will not be detectable to a system operator [8].

The evolution of attackers, attack methods and exploitable vulnerabilities clearly results in changing risks confronting smart grid security. The success of the attacks, detailed above, indicates that the security tools and applications, currently in use, are failing to protect critical infrastructures from advanced attackers. New tools and methodologies for both detecting and reacting to attacks are, thus, needed to fill the gap and limit the current threat landscape.

Much of the existing work on CPS security relies on the assumption that perfect knowledge of the physical system is available to the designer of the control and estimation system [2] or that the dynamics of the system can be modelled as discrete-time state transitions, using techniques such as Kalman filtering [9]. However, these methods are not always practical or accurate for complex systems with interdependencies between components, and can result in the use of over-simplified models which do not characterise the complexities and dynamics of the system well [9]. Furthermore, when the control system is based on a simplified system model, an attacker who can acquire sufficient knowledge of the system model may be able to generate an attack that will go undetected [8].

The smart grid already collects a vast amount of information that can be used to develop new security analytics tools to quickly and accurately detect cyber-attacks. These data allow the behaviour of the grid, under normal operating conditions, to be modelled. The detection of anomalies or deviations from normal behaviour, which may indicate attacks, is an important precursor to building resilient control systems, the final aim of which is to create critical infrastructures that repair or reconfigure themselves, in response to an attack. Apart from being able to spot obvious policy violations by applying *a priori* rules that compare measured data to thresholds or look for correlations across events, one possible feature in a consolidated security analytics tools could be assimilating diverse data sources to identify possible cyber-attacks that are invisible from the perspective of any one of these actions, but could be revealed by jointly considering several independent actions.

In this work, a framework for enhanced smart grid security is proposed, which enables anomaly detection by means of the joint implementation of various data analytics algorithms,

 ISBN: 978-1-61208-585-2

including methods driven by expert system knowledge and statistical analysis, as well as data-driven techniques from machine learning. The algorithms process the available data, intelligently exploiting the inherent redundancies in the system. The framework, called a Security Information Analytics (SIA) tool, is designed to be flexible, in order to allow other methods and algorithms to be incorporated over time.

The remainder of this paper describes the approach followed to develop the SIA tool for the smart grid. The threats faced in smart grid security, along with requirements and constraints for security analytics, are highlighted in Section II. This is followed by an introduction to the Nimbus testbed, which was used to develop and validate the SIA tool, in Section III. The paper continues with a description of the internal architecture of the SIA tool in Section IV. The preliminary results are outlined in Section V and some conclusions are discussed in Section VI.

II. Smart Grid Security

A. Smart Grid Threats

The NESCOR failure scenarios [10] are an extremely valuable resource for anyone trying to understand and mitigate potential cyber physical attacks against a smart grid environment. Scenarios are organized in terms of impact and each scenario addresses attacker profile, attack method and exploited vulnerability, as they are relevant to that particular scenario. The scenarios are organized into six domains:

1) Automated Meter Infrastructure (***AMI***)
2) Distributed Energy Resources (***DER***)
3) Wide Area Monitoring, Protection, and Control (***WAMPAC***)
4) Electric Transportation (***ET***)
5) Demand Response (***DR***)
6) Distribution Grid Management (***DGM***)

In this work, the focus is on the security of the meters, due to their importance in the smart grid infrastructure, considering, primarily, the NESCOR scenarios that are related to meter forgery and mass-disconnection attacks:

- ***AMI.1*** Authorized Employee Issues Unauthorized Mass Remote Disconnect: an employee within the utility, having valid authorization, issues a "remote disconnect" command to a large number of meters.
- ***AMI.9*** Invalid Disconnect Messages to Meters Impact Customers and Utility: a threat agent obtains legitimate credentials to the AMI system and issues a disconnect command for one or more target meters or schedules a disconnection to occur automatically at a later time.
- ***AMI.10*** Unauthorized Pricing Information Impacts Utility Revenue: a threat agent sends out unauthorized pricing information, such as Time-of-Use (TOU) pricing. This may result in either a loss or increase in utility revenue until the invalid price is recognized. Such an attack leaves the electricity supplier open to legal challenges from its subscribers.
- ***AMI.14*** Breach of Cellular Provider's Network Exposes AMI Access: inadequate security implementation in the AMI monitoring and control backup system allows a threat agent to execute an attack on the AMI implementation during a business continuity or disaster recovery scenario. Access to these backup systems allows a threat agent to perform malicious activity.
- ***AMI.32*** Power Stolen by Reconfiguring Meter via Optical Port: Many smart meters provide the capability of re-calibrating the settings via an optical port, which can be misused by economic thieves, who offer to alter the meters for a fee, changing the settings for recording power consumption and often cutting utility bills by 50-75%. This requires collusion between a knowledgeable criminal and an electricity customer, and will become widespread because of the ease of intrusion and the economic benefit to both parties.

B. Requirements and Constraints

In order to detect attacks, such as those outlined above, as well as unforeseen attacks, including those in which the attacker has gained knowledge of the ICS, the SIA tool aims to incorporate various different methods and algorithms, in order to provide a reliable and robust security solution for the smart grid. The primary requirements for such a system include the following:

- Minimise the probability of an undetected attack.
- Minimise the delay between the start of an attack and its detection.
- Minimise the probability of false alarm.

The first two requirements aim to reduce the impact of attacks by ensuring that interventions can take place immediately, minimising any financial losses, damage to physical components or danger to human life. Arguably as important as the first two requirements, minimisation of the false alarm probability avoids costly unnecessary interventions and, also, ensures that alerts are not ignored by operators. Secondary requirements include intuitive interfaces for visualisation and querying of data, integration into existing work flows, and allowing both real-time response and long-term investigations to be easily executed. However, these secondary requirements are considered to be outside of the scope of this paper.

There are many constraints that must be overcome in order to implement robust and reliable security analytics tools that will meet the afore-mentioned requirements. The dataset generated in the smart grid is very large and disparate, requiring massively parallel processing for a real time implementation. As such, any algorithms that are used, must be suitable for distributed processing and computational efficiency is an important consideration. The measurement precision of meters is limited and varies between devices, this can limit the potential for anomaly detection. Furthermore, when jointly considering the measurements from multiple meters throughout the system between the readings from different meters, synchronization, or the lack thereof, is a factor that must be carefully considered, in particular, for time-varying systems.

III. Introduction to Nimbus Testbed

The Nimbus Microgrid is a low-energy test bed commissioned by United Technologies Research Center (UTRC) in Cork, Ireland [11]. Along with an electrical microgrid, the test bed incorporates the thermal heating system of the Nimbus and Rubicon buildings of the Cork Institute of Technology,

 ISBN: 978-1-61208-585-2

to create a live-in laboratory for demonstrating building and climate controls.

A. Description

The Nimbus micro-grid (Figure 1) consists of the following components:

- A wind turbine
- A Li-Ion battery
- A combined heat and power unit
- A feeder management relay to couple the microgrid to the building grid
- A set of local loads

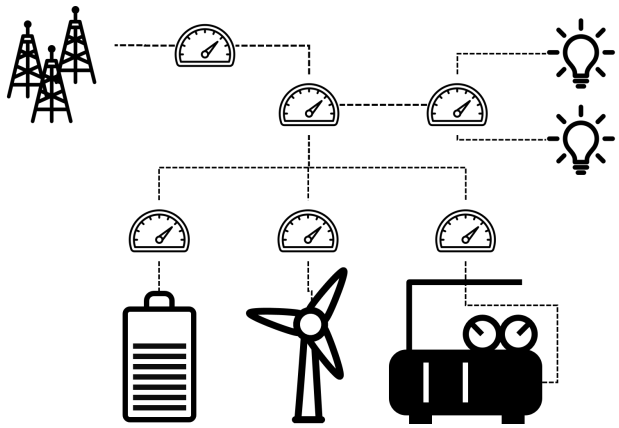

Figure 1. A simplified diagram of the Nimbus Test Bed

The microgrid and the connected thermal system are extensively monitored using a network of electrical meters and other sensors. These measurements, together with relevant information about gas and electricity power consumption measurements and prices, as well as thermal and electrical loads and weather and wind forecasts, are continuously available from the system and are collected into the data historian. The flow of information is outlined below.

B. Data Flow

1) **Measurement:** The primary points of data collection are the eight 3-phase electrical meters, each of which measures twenty-eight variables:
   - three phase-neutral and three phase-phase voltages,
   - four line currents (three phases and neutral),
   - total active ($\pm$), reactive ($\pm$), and apparent energy,
   - active, reactive and apparent power per phase,
   - total active and apparent power, and power factor,
   - frequency.

   The meter measurements make up the bulk of the collected data, accounting for a total of 224 variables. Furthermore, the battery, the combined heat and power unit, the wind turbine, the thermal storage tanks, and their associated inverters, all record the variables pertinent to each unit. These units also contain internal checks that generate alarms and warnings, which are communicated to the system.
2) **Collection:** The data variables listed above are communicated by the meters and system components to a programmable logic controller (PLC), which also logs other data from the system, such as the position indicators of all control valves and the status of breakers. It also acts as the conduit for the commands sent to the system, such as changes to the system mode and set points, commands to the breakers, as well as manual overrides. In total, 1252 variables are logged every second.
3) **Display & Logging:** The PLC communicates the data to the SCADA PC, which runs the human-machine-interface (HMI) tool shown in Figure 1, which displays the monitoring variables. The HMI also serves to display and acknowledge system alarms and warnings. The PC stores the variables into a database on the hard drive.
4) **Test Bed Middleware:** The Test Bed middleware is hosted on a PC on the same network as the SCADA PC. The middleware PC uses open platform communications (OPC) to periodically request the current variable values from the SCADA interface, which it parses and stores in another database on its hard drive. The middleware also acts the interface for any client (e.g., Matlab) to access the data using Simple Object Access Protocol.

IV. SIA Application

The SIA application is an interactive smart grid security analytics tool, implemented in R for the detection of anomalies in the Nimbus micro-grid. In this section, the architecture, algorithms used, and implementation of the tool are described in some detail.

A. SIA Architecture

The SIA application is composed of three main components: the security analytics engine, which tidies the SCADA data, runs the outlier algorithms, and makes a list of identified outliers; the web application, that visualizes the data and helps analysts to understand the security status of the grid; and a web API, an interface which can be used to feed security analytics intelligence into resilient control and remediation systems, to react to the threat or investigate the attack. This paper focuses on the security analytics engine.

B. Anomaly Detection Algorithms

There are five different methods of anomaly detection incorporated in the current implementation of the SIA tool and further methods will be added in ongoing work. The key idea behind the approach is to exploit redundancies, both in the data itself and in the outputs from the various methods, in order to improve the reliability of the anomaly detection.

The five currently implemented methods can be broadly categorized as *knowledge-based* or *data-driven*. The knowledge-based methods rely on expert knowledge of the micro-grid and its specific meters, or of the type of attack that might be carried out. For example, the voltage at any given meter is limited by the specifications of the equipment and the preconfigured value set by the test-bed operators. Similarly, a specific attack mode might cause multiple sensors to power off almost simultaneously; explicitly considering this type of attack can help it to be differentiated from a power fault. The *data-driven* category describes methods, such as machine learning, which rely on the data itself to learn the

 ISBN: 978-1-61208-585-2

normal behaviour of the system, with no explicit assumptions made about the source of the data or the relationships between variables.

The SIA application is comprised of the five anomaly detectors described below. The single-variable outlier detector, rule-based outlier detector and dead sensor clustering algorithm are considered to be *knowledge-based*, whilst the smart detector and Kullback-Leibler distance are considered to be *data-driven*.

1) Single-variable outlier detector: This outlier detector is the simplest implemented in the analytic engine. The detector identifies if the value of a measured variable falls outside of a predefined range for that variable. The threshold can be defined by known specification limits on equipment or operational thresholds. In this case, the thresholds were defined by the specifications of the meters used in the NIMBUS test-bed.

2) Rule-based outlier detector: The rule-based detector exploits redundancies in the measured variables to find anomalies. Each meter measures multiple closely related variables, some of which are not physically independent. As an example, consider the six different voltages measured by an electrical meter: the magnitudes of three phase-to-neutral voltages and three phase-to-phase voltages. Since only five independent variables exist in the voltage system (three magnitudes and two relative phases), it is evident that there is one exploitable redundancy: each voltage vector needs to form a triangle with two others to create a closed system, as shown in Figure 2.

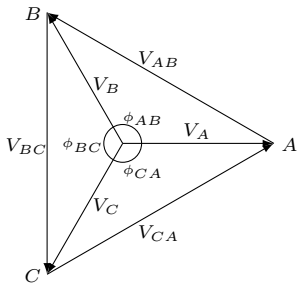

Figure 2. 3-Phase Voltage Phasors

Obtaining an equation from a redundancy requires expert knowledge. As an example, for Figure 2, Equation 1 sums the phases of the voltages:

$$\frac{1}{2\pi}\left[\cos^{-1}\frac{V_A^2+V_B^2-V_{AB}^2}{2V_AV_B} + \cos^{-1}\frac{V_B^2+V_C^2-V_{BC}^2}{2V_BV_C} + \cos^{-1}\frac{V_C^2+V_A^2-V_{CA}^2}{2V_CV_A}\right] = 1. \quad (1)$$

To account for measurement noise in the meter and other factors, such as sampling resolution and synchronization, historical data can be used to find the statistical distribution of the left hand side (LHS) of the equation. At any time, then, the value of the LHS for the current measurement can be compared to the historical distribution to calculate the probability of measuring that value. One or several thresholds can then be set on the probability that indicate the degree to which each redundancy check is violated.

In order to reduce false-positives, the number of violated equations is used as an outlier score. Namely, out of a total of twenty-one rules per meter, if less than three rules are violated, this is likely a false positive and can be safely ignored, however if more than six rules are violated the event is labelled as severe.

In order to remain portable, the system makes no assumptions about the variable output protocol or format. The equations are formatted using generic names for each variable. The rules are adapted to match the data format in use with a parsing routine. These rules can, then, be used directly with the input dataset.

3) Dead sensor clustering algorithm: This detector is designed to alert operators to the mass disconnection scenarios (***AMI.1***, ***AMI.9***, ***AMI.14***) discussed in Section II-A. This algorithm groups disconnected sensors using the time between disconnection. Multiple sensors in the same subnet work dropping within a few hours of each other likely points to an isolated hardware failure and poses a lower risk than a malicious attack. A much more severe event is a mass disconnection scenario where multiple related sensors receive a command to shut down within a few minutes of each other.

The dead sensor clustering procedure, illustrated in Figure 3, groups sensors into a cluster if they have disconnected within a time window which can be defined by the user. The time window is reset each time a sensor is disconnected and the cluster grows until no more sensors are disconnected within the time window. The cluster is defined as anomalous if the number of sensors associated with it is above a user-configurable threshold that should be defined in relation to the system size. This detector could be used to override a mass disconnection command and stop the attack at an early stage.

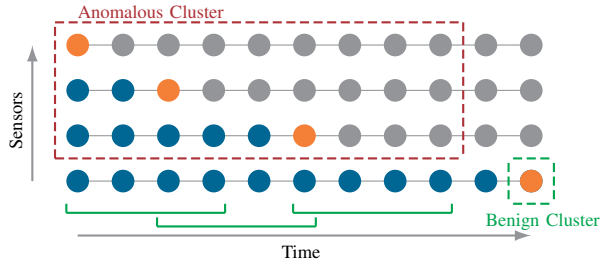

Figure 3. Diagram of the dead sensor clustering algorithm, showing the process by which disconnecting sensors are clustered together using a sliding time window. An orange node denotes a disconnected sensor, blue nodes denote connected sensors and grey nodes denote sensors that may be connected or disconnected. The time periods indicated in green represent the window. Here, a cluster with three or more sensors is considered anomalous.

4) Kullback-Leibler Distance: The Kullback-Leibler (KL) distance measures the difference between two distributions. In this case the symmetrized KL distance is used to determine by how much the daily measurements made by the sensors differ from a predefined baseline. Outliers are defined by those measurements which have a KL distance larger than a user-configurable value. In this work, the KL distance is calculated for each of the calculated rules, relating the redundant variables.

 ISBN: 978-1-61208-585-2

This detection algorithm serves to validate the results of the equations for an entire day against the baseline, and so it can not be used when running in real-time.

5) Smart Anomaly Detector: The so-called smart detector is a machine-learning (ML) algorithm that learns the normal behaviour of the system from the meter measurements to create a model. New measurements are, then, compared to the model and any instances which do not fit are classified as anomalous. In contrast to the rule-based anomaly detector, the smart detector produces a binary decision rather than a score.

ML algorithms are typically classified into supervised or unsupervised methods, depending on whether they require labelled data or not, respectively. Supervised methods typically work on data samples from two or more labelled classes, for example, normal and anomalous. The challenge with smart grids, and other anomaly detection exercises, is the lack of labelled anomalous data. In particular, it is very difficult to acquire known attack/fault data from smart grid installations and, even if such labelled anomalies were available, the case of new, unforeseen attacks or anomalies is not considered. One alternative is to assume that all data available represents normal behaviour, and to modify the supervised learning algorithm to work with a single class. Such algorithms are known as one-class ML, novelty detection, or anomaly detection algorithms in the literature. The algorithms learn the normal behaviour of the system, and then label any new data as anomalous if it does not fit with the model.

There are multiple anomaly detection ML algorithms in the literature, including variants of support vector machines (SVM), 1-Nearest Neighbour methods, parzen density estimation, and modified neural networks. In this work, a one-class support vector machine was used [12], [13], using the libsvm implementation [14]. Due to the diversity of electrical appliance behaviour, an individual model was trained for each meter in question. Some of the meters are connected to single-phase appliances while others to tri-phase industrial devices. As a result, some models include all variables used in the static rule-based detector, whilst others include a subset.

C. Combination of Anomaly Detector Outputs

The output from rule-based and smart anomaly detectors can be combined to reduce false-positives, by considering the overlapping subset of anomalous samples, detected by more than one detector. The single-variable detector is not included in the combination as it already provides an easily managable number of anomalies. In addition, this detector only examines a limited number of measurements, meaning the detection scope is much more restricted than the other detectors. This makes a combination with the single-variable detector inappropriate.

The combination is done by comparing the timestamps flagged as outliers by the smart anomaly detector and the rule-based detector. To get more information about which kinds of outliers are being detected by the smart detector, the overlap is examined as a function of the severity of the anomaly as defined in Section IV-B2.

V. Results

The results of the various outlier detection algorithms are visualized in the web application portion of SIA. However, here we present the results of the rule-based and smart anomaly detectors only as they highlight some of the constraints and challenges in developing an effective smart grid analytics system.

A day worth of data collected at the Nimbus testbed using a stable time resolution of 15 seconds is used here. Note that this resolution is described as stable as this granularity does vary within the time range. The varying time resolution must be considered when comparing results of different algorithms and examining the severity of an outlier.

The Nimbus micro-grid is composed of 8 smart meters; in Figure 4 a typical output from the outlier detectors is shown for a single meter. Note that only the single variable and rule-based detectors are included here. To address ***AMI.32***, high-risk rules are defined and highlighted to the operator. These are a subset of rules which contain electrical currents. The current has been chosen as a potential at-risk variable for manipulation by agents wanting to reduce the cost of electricity.

The total number of anomalies flagged by the rule-based detector in a single day is 20840 over all 8 meters. This volume of outliers is clearly too high for effective remediation. This highlights the need to either improve the detection algorithms to improve their performance, or combine these results with complementary methods to reduce the false positives.

The former requires a deep and specialized understanding of the system to more accurately model meter behaviour. This approach is both time consuming, and reduced the ability of the system to be utilized in a different environment.

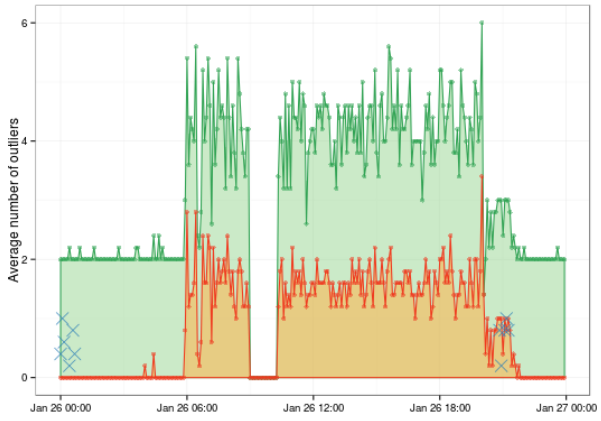

Figure 4. Number of outliers flagged as a function of time. Shown are the results from the rule-based and single variable detectors for a single sensors over a period of one day. The dotted distributions correspond to the number of outliers detected by the rule-based detector. The green distribution corresponds to all rules, while the red corresponds to so-called high-risk rules only. Anomalies detected by the single variable detector are marked by crosses.

Here, a combination of the rule-based detector and the smart anomaly detector results as described in Section IV-C is presented.

Examination of a days worth of data shows that a combination reduces the outliers by 70% compared to the rule-based detector alone. In addition, the combination filters out 80% of the low severity outliers while keeping over 93% of high severity outliers (Table I).

 ISBN: 978-1-61208-585-2

TABLE I. OVERLAP OF SMART AND RULE-BASED DECTORS BY SEVERITY

Severity	Overlap (%)
Low	17.7
Medium	56.2
High	93.7

VI. Conclusion and Future Work

The ever evolving security landscape presents a very real threat to critical infrastructure such as the smart grid. New technologies and modes of operation are required to protect the smart grid from increasingly sophisticated attacks. Exploiting data analytics is key in this effort. An overview of the design constraints for a security data analytics framework were presented along with a concrete implementation. The SIA application consists of an analytics engine designed to detect different attack and failure scenarios, and a web application interface to facilitate operations. Five anomaly detection algorithms were presented. These reflect both current approaches, relying on pre-existing knowledge and assumptions, and new approaches, that depend on data to create models with minimal domain-specific knowledge. Measurements from the microgrid are affected by multiple effects, which as a whole, limit the performance of the rule-based approach. In order to reduce false positives, a combination with an ML-based detector was carried out with some success. Remedying the limitations of the rule-based approach would require a greater understanding of the specific measurement components, and lead to an overspecification of algorithm. This would require significant work and reduce the applicability of such a model to other systems. Smart detectors which learn the behaviour of the system from the data can detect anomalies making minimal assumptions about the kinds of attack patterns, making the system more secure against future threats.

Acknowledgment

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 608224.

References

[1] D. Zhaoyang, “Smart grid cyber security,” in Control Automation Robotics Vision (ICARCV), 2014 13th International Conference on, Dec 2014, pp. 1–2.

[2] A. Jones, Z. Kong, and C. Belta, “Anomaly detection in cyber-physical systems: A formal methods approach,” in Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on, Dec 2014, pp. 848–853.

[3] A. Cherepanov. BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry. [Online]. Available: http://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/ (2016)

[4] J. Nazario, “Blackenergy ddos bot analysis,” Arbor Networks, 2007.

[5] J. Hultquist. Sandworm team and the ukrainian power authority attacks. [Online]. Available: http://www.isightpartners.com/2016/01/ukraine-and-sandworm-team/ (2016)

[6] S. R. Symantec. Sandworm windows zero-day vulnerability being actively exploited in targeted attacks. [Online]. Available: http://www.symantec.com/connect/blogs/sandworm-windows-zero-day-vulnerability-being-actively-exploited-targeted-attacks (2014)

[7] S. S. Response. Cyberespionage attacks against energy suppliers, version 1.21. (2014)

[8] Y. Yuan and Y. Mo, “Security in cyber-physical systems: Controller design against known-plaintext attack,” in Decision and Control (CDC), 2015 IEEE 54th Annual Conference on, Dec 2015, pp. 5814–5819.

[9] F. Pasqualetti, F. Dörfler, and F. Bullo, “Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design,” in Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on, Dec 2011, pp. 2195–2201.

[10] National Electric Sector Cybersecurity Organization Resource (NESCOR), workgroup 1. National electric sector cybersecurity organization resource (nescor). (2014)

[11] V. Valdivia, S. O’Connell, F. Gonzalez-Espin, A. E. din Mady, K. Kouramas, L. D. Tommasi, H. Wiese, B. C. Villaverde, R. Foley, M. Cychowski, L. Hertig, D. Hamilton, and D. Pesch, “Sustainable building integrated energy test-bed,” in Power Electronics for Distributed Generation Systems (PEDG), 2014 IEEE 5th International Symposium on, June 2014, pp. 1–6.

[12] B. Schölkopf, A. J. Smola, R. C. Williamson, and P. L. Bartlett, “New support vector algorithms,” Neural Comput., vol. 12, no. 5, May 2000, pp. 1207–1245. [Online]. Available: http://dx.doi.org/10.1162/089976600300015565

[13] B. Schölkopf, J. C. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson, “Estimating the support of a high-dimensional distribution,” Neural computation, vol. 13, no. 7, 2001, pp. 1443–1471.

[14] C.-C. Chang and C.-J. Lin, “Libsvm: A library for support vector machines,” ACM Transactions on Intelligent Systems and Technology (TIST), vol. 2, no. 3, 2011, p. 27.

 ISBN: 978-1-61208-585-2