Context-Awareness Using Anomaly-Based Detectors for Smart Grid Domains

Cristina Alcaraz(✉), Lorena Cazorla, and Gerardo Fernandez

Computer Science Department, University of Malaga,
Campus de Teatinos S/n, 29071 Malaga, Spain
{alcaraz,lorena,gerardo}@lcc.uma.es

Abstract. Anomaly-based detection applied in strongly interdependent systems, like Smart Grids, has become one of the most challenging research areas in recent years. Early detection of anomalies so as to detect and prevent unexpected faults or stealthy threats is attracting a great deal of attention from the scientific community because it offers potential solutions for context-awareness. These solutions can also help explain the conditions leading up to a given situation and help determine the degree of its severity. However, not all the existing approaches within the literature are equally effective in covering the needs of a particular scenario. It is necessary to explore the control requirements of the domains that comprise a Smart Grid, identify, and even select, those approaches according to these requirements and the intrinsic conditions related to the application context, such as technological heterogeneity and complexity. Therefore, this paper analyses the functional features of existing anomaly-based approaches so as to adapt them, according to the aforementioned conditions. The result of this investigation is a guideline for the construction of preventive solutions that will help improve the context-awareness in the control of Smart Grid domains in the near future.

Keywords: Smart Grid · Control systems · Context-awareness · Prevention

1 Introduction

Anomaly-based detection has become one of the most challenging research areas within critical infrastructure protection in recent years, despite its extended application in intrusion and fault detection in conventional systems. There are a multitude of anomaly-based techniques for prevention available [1–3], but not all of them are equally feasible for critical contexts where the networks are extremely complex, dynamic and strongly-interconnected. Any perturbation in the functional requirements of these systems can seriously affect not only the underlying infrastructures but also those interdependent networks themselves. This is the case of Smart Grid systems, which are based on seven chief domains: control systems, energy (production, transmission and distribution) substations, providers,

J. Lopez et al. (Eds.): CRiSIS 2014, LNCS 8924, pp. 17–34, 2015.
DOI: 10.1007/978-3-319-17127-2_2

market and end-users. In this context, the operational tasks related to monitoring, supervision and data acquisition become fundamental to the correct use of the power grid. This also means that any inaccuracy in the detection processes of anomalies, computational overhead or a misunderstanding of the situation can trigger a (slight or serious) change in the control of the entire grid, and therefore cause an undesirable or contrary effect in its stability.

We therefore explore in this paper those anomaly-based approaches that can be found in the current literature, so as to evaluate their functionalities and applicability in the context of Smart Grids, paying particular attention to those conditions that entail a degradation in control. These conditions are related to a set of requirements associated with the monitoring and security of the entire Smart Grid, and the natural conditions of the communication infrastructures. The result of this investigation is a guideline to which approaches are most suitable for each section of the grid related to the control, such as substations. Thus, we contribute with the means necessary to help those responsible members for the control of the grid, such as human operators/engineers or network designers, and even researchers, define and implement future effective solutions for context-awareness. The paper is organized as follows: we briefly review in Sect. 2 the control technologies and communication infrastructures in order to then decide in Sect. 3.1 what requirements have to be fulfilled by the existing anomaly-based approaches. The functionalities and functional features of these approaches are discussed in Sect. 3.2 to later look at their suitability in control contexts (in Sect. 4) before concluding with a discussion of our findings and on-going work in Sect. 5.

2 General Architecture and Technologies

An introduction to the communication infrastructures and technologies that comprise a Smart Grid is given in this section [4]. The central architecture of these systems corresponds to a decentralized control network capable of remotely communicating with the rest of the sub-domains of the Smart Grid, e.g., substations. At this point, smart meters, gateways, Remote Terminal Units (RTUs), sensors and a set of control objects interact with each other through large and small communication infrastructures such as backhaul, Wide Area, Field Area, Neighbourhood Area, and Local Area Networks (WANs, FANs, NANs and LANs, respectively). All these infrastructures base their communications on wired and wireless systems such as mobile cellular technology, satellite, WiMAX, power line communications, microwaves systems, optical fiber, Bluetooth, Wi-Fi, Wireless Sensor Networks (WSNs), Ethernet, and so on. These infrastructures are in charge of distributing monitored evidence (e.g., commands, measurements or alarms) occurring at any point of the Smart Grid system, where backhaul and the Internet are the chief infrastructures that connect the different sub-domains with the rest of the networks, including Advanced Metering Infrastructures (AMIs). An AMI is a bidirectional interface with the capability to manage and interact with smart meters and utility business systems, thus substituting the traditional one-way advanced meters.

This interconnection map primarily focuses on the secure monitoring of services and the effectiveness of energy production according to the real demand. These services mainly addresses the means of notifying electricity pricing at any time and provide the end-users with customizable services to efficiently manage energy consumption. Continuing with the topic of monitoring services, the control transactions between the control system and substations are led by communication interfaces (e.g., RTUs, gateways, servers, etc.) which serve as intermediary nodes between the remote substation and the Master Terminal Units (MTUs) of the central system. An RTU is a device working at ∼22 MHz–200 MHz with 256 bytes–64 MB RAM, 8 KB–32 MB flash memory and 16 KB–256 KB EEPROM. These hardware and software capabilities are enough to compute data streams, operate mathematical formulations and identify those sensors or actuators in charge of executing a specific action in the field. These interfaces are also able to establish connections with other substations, allowing an inter-RTU communication with the ability to ensure store-and-forward using one of the two existing communication modes, serial (e.g., IEC-101) or TCP/IP (e.g., Modbus-TCP).

Control objects can be classified according to the type of micro-controller (weak, normal, and heavy-duty), the type of radio transceiver (wideband and narrowband radios) and the type of communication (synchronous/asynchronous) [5]. Within the category weak, we find those limited devices such as home-appliances and sensors with extremely constrained capabilities such as ∼4 MHz, 1 KB RAM and 4 KB–16 KB ROM, but with sufficient capacity to execute simple applications. Conversely, those classed as normal are those nodes that are able to comply with any kind of collaborative network. A node belonging to this category usually has a micro-controller of ∼4 MHz–8 MHz, 4 KB–16 KB RAM and 48 KB–256 KB ROM. Finally nodes belonging to the heavy-duty category are expensive devices (e.g., handled devices) that are able to execute any simple or complex critical application. Their microprocessors are quite powerful working at around 13 MHz–180 MHz, 256 KB–512 KB RAM and 4 MB–32 MB ROM. With respect to transceivers, most of the sensory devices follow the IEEE-802.15.4 standard working with wideband radios (e.g., CC2420) at frequencies of 2.4 GHz with certain demand restrictions in power. The narrowband radio-based transceivers (e.g., CC1000/C1020), to the contrary, work at lower frequencies and are more susceptible to noise, but they have less power consumption and faster wake up times.

Within the heavy-duty class, we highlight the industrial WSNs which are normally deployed close to critical systems (e.g., generators, transformers, pylons, etc.). Their capabilities are slightly greater than the conventional ones equipped with a ∼4 MHz–32 MHz micro-processor, 8 KB–128 KB RAM, 128 KB–192 KB ROM, and specific sensors to measure physical events associated with the industrial context such as temperature, voltage load, etc. They have the possibility to be directly linked to energy suppliers or industrial equipment in order to maximize their lifetime with self-capacity for processing and transmitting measurements to a base station (e.g., a gateway or an RTU). With similar features, smart meters can become heavy-duty devices working at ∼8–50 MHz, 4 KB–32 KB RAM and 32–512 KB flash memory. An electrical meter is a device capable of logging the consumption values in synchronous and frequent intervals, sending this information back to the control utility for monitoring and billing purposes. Depending on the type of network, the communication can also vary [4]. For example, in power generation, transmission and distribution substations the communication can depend on specific or property protocols such as IEC-61850, Modbus, Zigbee, WirelessHART, ISA100.11a, and so on. Many of these offer technical solutions for customizing and optimizing the conditions of the application context in order to improve its quality of service, or avoid, for example, industrial noise, interferences or obstacles.

3 Detectors: Requirements and Common Approaches

Given that the great majority of the control objects (e.g., sensors, smart meters, etc.) are distributed over large-scale distributions where the control generally relies on only a few (or perhaps none) human operators in the field, topics related to dynamic and reliable context-awareness solutions should therefore be considered. Specifically, we explore a set of existing anomaly-based techniques as a support to these solutions. But as the number of techniques is significant within the current literature, we also stress here primary requirements and conditions that such techniques should comply with so as to ensure a better prevention in critical systems contained within a Smart Grid.

3.1 Requirements for Anomaly-Based Detection

The concept of 'context' was introduced by A. Dey in [6] as "*any information that can be used to characterize the situation of an entity*", where entity can be a person, place or object. This characterization is widely used by dynamic context-aware computing systems to detect, prevent and alert to unforeseen changes in the normal behaviour of the system being observed [7]. An example of these detection systems are the Intrusion Detection Systems (IDSes), the configurations of which should respect the intrinsic requirements of the control not to perturb the normal behaviour of the entire grid. These requirements are as follows:

- *Operational performance* ([**R1**]) is part of the control of a Smart Grid. This includes the availability in-real time of assets and data from anywhere, at any time and in anyway; in addition to ensuring a fast supervision, data acquisition and response, avoiding communication and computational delays as much as possible.
- *Reliability and integrity* in the control ([**R2**]). Any change in the system can cause serious deviations in the power production and distribution, putting the stability of the power grid at risk.

- *Resilience* ([**R3**]) to address anomalies or unexpected incidents, which might also come from intrusive actions. Likewise, aspects related to *security* ([**R4**]) at the different levels of the communication and architecture must therefore also be considered as primary requirements for resilience.
- As part of the security, data confidentiality and anonymity are requirements required to guarantee *privacy* ([**R5**]) of both users and utilities.

Working within these requirements, anomaly-based detectors need to ensure a set of conditions to guarantee a fast, integral and reliable monitoring of evidence. That is to say, detectors need to show their potential to quickly find pattern sequences that prove the existence of a deviation within a set of data instances; i.e.:

- Low computational complexity through optimized algorithms and handling of parameters, in addition to guaranteeing a speedy classification, learning and comprehensibility of the data instances. In this way, it is possible to meet the operational requirement ([**R1**]).
- Reliability through accurate detection with a low false positive/negative rate, comprehensibility of the results obtained, easiness to handle parameters, and tolerance to highly interdependent data, noise, missing values or redundancy. The idea is to offer the best way of understanding a situation so as to act accordingly ([**R2**]).
- Capacities for incremental learning to update the knowledge of the system with new (discrete/continuous) values, states, threat patterns or parameters. This will permit the underlying infrastructures to provide an updated protection layer for survivability (security and resilience against future threats, [**R3, R4, R5**]).
- Ability to control drastic or persisting changes in the normal behaviour of the system, as these deviations can mean the proximity or existence of intrusive actions, affecting [**R3, R4, R5**].

Taking all this into account, we explore and analyse the functional features of the existing anomaly-based approaches to evaluate their functionalities according to the fulfilment of the requirements given for the application context.

3.2 Context Awareness Through Anomaly-Based Detection

Given that there are so many techniques available in the literature, and we are interested in detecting single anomalies that can cause significant damage to critical systems, we concentrate all our attention on the surveys carried out by M. V. Chandola et al. in [1] and S Kotsiantis et al. in [2], and on the taxonomy given by Gyanchandani et al. in [3]. Examining these three papers, we explore functional features to later discuss the suitability of the existing techniques in the Smart Grid context.

Data Mining-Based: this classification defines a type of analysis which is carried out on a set of data to find the behaviour pattern sequences, such as:

- **Classification-based** techniques: these correspond to classifiers in charge of assigning data instances to (normal or anomalous) classes [1]. Within this category, the **decision trees** (e.g., ID3, C4.5) are the most representative structures which deal with mapping observations into conclusions using hierarchical rules under the assumption of 'divide and conquer'. This assumption consists of recursively breaking down a problem into sub-problems until these become atomic units. There are two types of decision trees: *classification* and *regression* trees, the results of which depend on the type of data managed and the desired outputs of the models. These tree-like structures are capable of providing fast computations and decisions since each data instance (in the testing phase) is compared against a precomputed model. Their advantages are the speed of classification and the comprehensibility degree of their outputs to humans. Nonetheless, their shortcomings are the tolerance to redundant or highly interdependent data, as well as, their reliance on predefined models primarily based on labels [2,3].
- **Association rule learning-based** techniques: unsupervised schemes which try to identify the relationships between categorical variables, using strong rules and thresholds to prune. As part of this classification, we highlight the *Apriori* algorithm and the *FP-growth* algorithm. The former is an influential algorithm for mining frequent patterns, which tries to find rules in large datasets to predict the occurrence of an item based on the occurrences of others. In fact, its main property is: "any subset of a frequent pattern must be frequent"; and its pruning principle is "if there is a pattern which is infrequent, its superset should not be generated". Similarly, FP-growth has the same goals, but uses a compact frequent-pattern tree (FP-tree) structure under the assumption of 'divide-and-conquer'. This assumption consists of finding frequent rules/patterns to decompose mining tasks into smaller ones, the aim of which is to recursively delete all the data items that are not frequent; instead of generating candidates for each study. As mentioned, the technique itself has to make use of pruning approaches to reduce the sets of rules. Hence, the effectiveness of the learning process depends heavily on the parameters that configure the pruning operations and their algorithms, and on the number of rules that have to be launched, where the processing time may increase exponentially regarding the number of attributes [3]. Nonetheless, the comprehensibility of the results is an advantage.
- **Clustering-based** techniques: these aim to classify data instances in clusters through an unsupervised or semi-supervised method; i.e., no knowledge of threats, attacks or anomalies are needed in advance during training. This feature helps the testing phase process the evidence quickly, where the unsupervised models only compare the instances with a small number of clusters. To do this, the technique needs an evaluation function (e.g., a distance function, density, etc.) to compute the distances between data points, where each instance is evaluated according to its entire cluster. Although there are several

clustering algorithms (e.g., hierarchical, centroid-based, distribution-based, density-based, etc.), the most popular approach is the *k-means*. Clustering-based techniques are quite dependent on the algorithm's parameters, which consequently have associated computational costs, which are mainly influenced by the type of dataset and the parameters selected [1,8]. Most approaches follow a quadratic order, except those based on heuristics (e.g., k-means), which take a linear complexity. In addition, the tolerance of the algorithms to different constraints in the data are quite dependent on the configuration of the parameters selected [1].

Statistical-Based: this class defines those statistical techniques that compute statistical models to apply interference tests so as to verify whether or not a specific instance belongs to a statistical model. Within these techniques, it is possible to find:

– **Parametric and nonparametric-based** methods: these refer to inference engines with a strong dependence on the data observed and which are composed of well-known statistical models, such as Gaussian or histograms [1,8]. These statistical models are in general accurate and tolerant to noise and missing values. Additionally, the statistical analysis provides additional information to the detection systems, such as the confidence interval associated with the anomaly. However, depending on the dataset, these methods can be sensitive to subtle changes and the output results are difficult for humans to understand. Moreover, depending on the dynamics of the problem, the efficiency of the model can be reduced, and in some cases, these techniques can potentially have quadratic complexity if dealing with large databases [1]. In contrast, the chief disadvantage here is that these techniques assume that the production of the data follows a particular distribution, which in real life scenarios is not true [1], consequently there are difficulties in determining the best distribution to fix such data. This category also includes the **operational models**, the observations of which are evaluated according to counters, bounded by predefined (upper and lower) thresholds. If these boundaries are not efficiently computed, the approach itself can then hamper the dynamic detection of anomalous events. In general, operational models may not be suitable for those dynamic scenarios that regularly change their normal behaviour [3].

– **Time series-based** techniques: these, can be both non-parametric and parametric [9], basically aim to provide behaviour forecasting using times series, which are sequences of data points, measured at successive and uniformly distributed time intervals. These methods are generally suitable for detecting those threats launched in series form with subtle perturbations (e.g., stealth attacks), but its effectiveness decays when there are drastic changes [3]. There are several methods of time series analysis; one of the most useful for detection are the *smoothing techniques*, which provide weighted data instances. The smoothing mechanisms provide accurate observations and their approaches are tolerant to insignificant changes and missing values, in addition they help optimize parameters. Unfortunately, as in the case of the rest of the statistical methods, they tend to be difficult to understand for humans and have great difficulty handling parameters. The smoothing techniques also produce weak models for medium or long-range forecasting, which heavily rely on past history and on the smoothing factor to predict the future; the variant *exponential smoothing models*, in particular, cannot easily forecast future events in the presence of fluctuations in recent data [10].

- **Markov models**: are mathematical representations with quantitative values that help predict the future behaviour of a system according to the current evidence. There are many types of Markov models, and all them have functionalities and features in common, such as operations based on successive data and dependence on a state transition (probabilistic) matrix to illustrate activity transactions without having knowledge of the problem in hand. However, and unfortunately, the Markov models are highly complicated when addressing complex situations with multiple dimensions, the complexity of which increases when leaving the most simple (first order) Markov chains, in favour of more precise and complicated models [11] (e.g., the Hidden Markov Models (HMMs)). In addition, abrupt changes in the normal activity sequence within a system becomes unmanageable, so that this feature may become undesirable in critical contexts [3].

Knowledge Detection-Based: this technique consists of progressively acquiring knowledge about specific attacks or vulnerabilities, guaranteeing accuracy of the technique with a low false positive rate, and flexibility and scalability for adding new knowledge. The result is a system potentially capable of ensuring resilience against threats, but this security also depends on the update frequency of this knowledge and the degree of granularity to specify the threat patterns. According to M. Gyanchandani et al. in [3], there are a few types of knowledge detection-based approaches, such as state transition, expert systems and Petri nets. **State transactions** aim to define threat models through state transaction diagrams illustrating the activity sequences and operandi mode; similarly, **Petri nets** represents state transactions using directed bipartite graphs to show events and conditions. Conversely, **expert systems** are composed of intelligence engines based on simple rules which define different models capable of reasoning about the provided knowledge like a human expert. Expert system models can be provided with varied knowledge; e.g., different types of threats or vulnerabilities, or even conditions given by the security policies.

Information and Spectral Theory-Based: both theories are based on statistical approaches. Particularly, the information-based techniques focus on analysing the data itself and its order to observe whether there are irregularities (related to meaning, features or properties) within it [1]. Through concepts of entropy, their approaches are in general efficient, but this feature depends on the size of the dataset to be compared; and they are also tolerant to insignificant changes in the data and redundancy [14]. As for spectral theory methods, these work with approximations of the data (or signals) to observe whether there are differences, more visible in other dimensions of the data. Spectral analysis is an approach fairly linked to time series analysis and the characteristics of the communication channels. It performs dimensionality reduction to handle high dimensional data; however, its efficiency varies according to the mathematical method used to translate the model into other dimensions, e.g., Fourier, and these techniques usually have a high computational complexity [1].

Other Machine Learning-Based: in this group, we stress the rest of machine-learning-based approaches [15] such as artificial neural network or Bayesian networks, amongst others. Note that the vast majority of these techniques overlap with other aforementioned ones, such statistical or mining data.

- **Artificial neural networks** (ANNs): these, in the artificial intelligence field, can be applied for anomaly detection using a multi-class or one-class configuration for training and learning. The models essentially consist of the computation of the sum of weighted inputs to produce weighted outputs [2]. Thus, the performance of ANNs depends on three main aspects: input and activation functions, network architecture and the weight of each connection. ANNs are generally accurate and fast classifiers, capable of tolerating highly interdependent data, whose learners can need of back propagation algorithms where the output models may not be comprehensible to humans and produce over-fitted models. These drawbacks make it difficult to ensure real-time in the operational processes since most ANN approaches need extra processing-time.
- **Bayesian networks** (BNs): these networks are composed of directed acyclic graphs, where the nodes represent states that have associated probabilities, and parameters encoded in tables. The BN first learns from structures of the (either unknown or known) networks, and then computes the parameters of the model. This category can be well-applied in intrusion detection models as powerful and versatile solutions, but may become computationally complex if the networks are unknown a priori [2], or present too many features (large BNs). Despite its ideal accuracy, this technique is too expensive in terms of time and storage, and tends to be infeasible for constrained scenarios. An extension of BNs are the **Naïve Bayes networks**, where their digraphs only hold one parent for each node and the probabilistic parameters of the network are calculated using conditional probabilities. These types of probabilities in the form of a product can be transformed into a sum through the use of logarithms, allowing the decision system to be computationally efficient and fast [2]. Other benefits, given the simplification of the model, are the diminished computational overhead for training, understandability of their networks, and the possibilities for handling parameters and introducing incremental learning. However, a disadvantage of this model is that it is not as accurate as a BN due to the existing independence between the child nodes, which imposes strong constraints on its behaviour [2].
- **Support vector machines** (SVMs): this method is a supervised learning model based on a non-probabilistic binary linear classifier under a one-class

configuration to recognize data patterns or outliers in datasets [12]. Given that SVMs work with linear combination of (data) points, the computational cost follows a quadratic order and the number of vectors selected is usually small. Thus the complexity of an SVM is not affected by the number of features in the training data so SVMs are suitable for addressing large numbers of features. The main weaknesses found is that most real-world problems involve inseparable data for which no hyperplane exists that successfully separates the positive from negative instances in the training set; and in optimization problems, the presence of local minimums and maximums affects the accuracy and speed. Even so, SVMs are, in general terms, accurate and fast classifiers, and tolerant to irrelevant and redundant data. However, the method itself usually presents problems with the speed of learning, the comprehensibility and the ability to handle the model and incrementally learn [2].

- **Rule-based techniques**: these focus on learning rules that interpret the normal behaviour of the system with the capability of multi-class and one-class settings. Their main strengths are the accuracy, comprehensibility, handling of simple parameters and low complexity. In contrast, they are weak in incremental learning, dependence on expert knowledge, tolerance to noise and are unsuitable for anomaly detection. Within this class, we highlight the **rule learners** (e.g., Ripper). These algorithms use rules from trained data to construct a rule-based decision engine under the assumption 'separate and conquer' by looking at one class at a time and producing rules that match the class. This procedure, apparently simple, requires exploring the whole dataset where their learners become slow and inaccurate with low tolerance to missing irrelevant and redundant data. Nonetheless, they provide speedy classifiers with comprehensible results, and allow easiness to manage system parameters.
- **Nearest neighbour-based**: this corresponds to those methods based on the distance measures of the data, such as the k^{th} *nearest neighbour* or on the *density*. These approaches are characterized by their speedy learning with respect to the number of attributes and the number of instances present in the dataset. In addition, they are suitable for incremental learning and their parameters can be modified with fairly easily. Despite these benefits, these approaches are quite sensitive to the selection of the similarity function [8], do not provide a deterministic way of choosing the parameter$k$, and require storage. The size of the instance sets are also dependent on k whose value affects the time required to classify an instance; in addition to exhibiting an extensive testing phase in which their methods can reach a low tolerance to noise and a low stability depending on the parameters adjusted.
- **Fuzzy logic** and **genetic algorithms**. Fuzzy logic consists of simple rule-based structures that define reasoning [3]. The approaches are in general simple, flexible and fast in the processing of rules and in the determination of anomalies, in which their approaches are able to establish the normality boundaries and manage large databases. The technique is also able to model complex systems and situations without requiring precision or complete databases; however, its conclusions may not reflect the confidence degree of a

problem. Regarding genetic algorithms, these deal with optimization and search heuristics where their implementations can require a large number of iterations to reduce a problem, and according to a fitness function. This also means that the detection rate depends on the accuracy of this function, where the approach itself has proven be unable to detect unknown or new threats, as well as, multi-interactive attacks [13].

Table 1. Work related with approaches applied in Smart Grid environments

Reference	Technique	Application	Application area
[16]	ANNs	Fault diagnosis	Substations
[17]	Decision trees	Intrusion detection	Control and substations
[18]		Fault detection	Substations
[19]	BNs	Intrusion detection	HANs
[20]	Naïve Bayes net	Islanding detection	Power systems
[21]	SVMs	Fault detection and classification	Transmission lines
[22]		Intrusion detection	HANs, NANs, WANs
[23]	Rules	Intrusion detection	WANs, NANs and HANs
[24]	Statistical	False-data injection detection (Markov graph-based)	Control and substations
[25]		Load/Price Forecasting, Demand (time series)	HANs, Control and substations
[26]	Fuzzy logic	Diagnosis and maintenance	Substations
[27]		Optimization for power storage	Microgrid networks
[28]	Petri Nets	Fault diagnosis	Distribution substations
Examples of combined solutions			
[29]	ANNs and rules	Fault diagnosis	Control and substations
[30]	BNs on an expert system	Fault diagnosis	Substations (distribution feeder)
[31]	Fuzzy logic and decision tree	Islanding detection	Substations

To ensure these techniques are effective, they can be integrated inside intrusion detection systems to monitor and analyse events following one of the three detection modes: **anomaly-based** (to detect unexpected deviations regarding the normal behaviour of a system), **signature-based** (to detect changes according to an updated database containing threat models) and **specification-based** (to detect abnormal behaviours taking into account the legitimate specifications of a system). According to P. Jokar in [19], anomaly-based IDSes have a tendency towards high false positive rates, complex training and tuning time, but they do have the ability to detect unknown attacks. Signature-based IDSes present low false positive rate but they are not able to detect unknown threats; whereas specification-based IDSes ensure low false positive rates and have the capability to detect new attacks. Nonetheless, specification-based IDS presents great disadvantages related to the computational cost required implementing the threat/vulnerability models, which are very dependent on the functional features of the devices (legitimate specification). Table 1 summarizes some related work so as to show the extensive application field of these techniques: monitoring, detection, optimization and maintenance.

4 Suitability of Detection Approaches for Smart Grid Domains

In this section, we explore several ways to select anomaly-based techniques. To do this, Table 2, summarizes the functional benefits of each scheme analysed in Sect. 3.1, but compared against the control and security conditions stated in Sect. 3.1 and the characteristics of the communication systems (dimension, traffic and capabilities of the network devices).

4.1 Utilities: Control Centres and Corporate Networks

Control and corporate networks of a Smart Grid may range from large distributions with potentially thousands of nodes (e.g., servers) with connections to backhauls, WANs or NANs, to small and local networks. Depending on the type of domain and utility, they may have different kinds of protocols and topologies to connect different networks (e.g., control and AMI, providers and AMI). However, this interconnection mode and its relation to public networks, like the Internet, forces us to consider heavy-duty IDSes that help detect potential (anonymous, unknown, concurrent or stealthy) threats, and thereby comply with the minimum security requirements [**R3, R4, R5**]. As part of this information belongs to users or the business itself, and the other part corresponds with control transactions for the protection and stability of the entire power grid, topics related to reliability of the data itself [**R2**] should also be considered. Therefore, and observing Table 2, the most suitable techniques for this section of the grid could be:

- **Knowledge-based**: the dynamic features of the knowledge-based approaches, such as expert systems, make them be one of the most attractive approaches to be applied in complex and dynamic contexts. However, this protection will highly depend on the degree of granularity of their knowledge and the frequency to with which this knowledge is updated; two conditions that should be well-specified in the security policies.
- **Statistics**: statistical-based techniques, as described in Sect. 3.2 are powerful methods that can be adapted to different scenarios, from simple to complex and dynamic contexts, and serve as anomaly-detection engines in multiple IDSes in the literature [1,8]. Statistical methods could be useful for detection at any level of a communication network because of their great accuracy

(except the operational models) despite being computationally complex. Note that the **Markov models** may also be considered due to their inherent characteristics, but their transaction matrices should be well-fixed to control drastic changes. Specifically, HMMs are useful tools for detecting hidden dynamics and extracting knowledge when there are gaps in the information received. Thus in the presence of encrypted traffic, the use of Markov models would be useful to detect certain hidden evidence ([**R3, R4**]).

As mentioned, there are other methods that could equally be applicable to theses types of networks, e.g., rule learners, SVMs, Markov models or clustering techniques. However they could be more difficult to adapt to the scenario, or present more challenges and inconveniences than benefits due to their inherent characteristics. For example, these methods tend to produce over-fitting, a characteristic that makes them inappropriate when the environment is continuously adapting new dynamics and new constraints (e.g., frequent upgrades and maintenances). As for the detection modes, the use of a **signature-based IDS** seems to be a good option since utility networks might apply existing and complex databases with diverse types of signatures defining threat patterns or known undesirable dynamics related to the network. The main problem found in this detection mode is the need to keep the threat databases up-to-date.

4.2 Substations: Production, Transmission and Distribution

The communication between the control centre and the remote nodes (i.e., RTU/gateway) is done through MTU, where the data traffic between the MTU-RTU/gateway is generally regular and standardized, and operational performance ([**R1**]), reliability in the control transactions ([**R2**]) and security ([**R3, R4**]) are all required. As mentioned in Sect. 2, RTUs are powerful enough to be able to execute a set of operations or instructions, as well as, advanced algorithms such as machine learning ones. Their hardware capacities also allows them to run specialized detection techniques capable of detecting sophisticated threats in an environment that has a regular behaviour with a monotonous activity (note that this consideration is dependent on the security policies). Assuming that the communications are configured to be synchronous with regular traffic, the most suitable techniques for this section of the grid would be those related to **knowledge**. However, and as described above, the implementation of knowledge-based systems also depends on the functional features of the interfaces and the maintenance of these intelligent systems. As an alternative, it is also possible to choose those approaches that do not infringe, at least, [**R1, R2**] to ensure control at all times, such as:

- **Rule-based techniques**: this method is characterized by its simplicity ([**R1**]) and accuracy ([**R2**]), which should not degrade the main conditions for control. For the effectiveness of the approach and its use for protection, it is necessary to specify in detail, the rules, exposing all the possible threat scenarios that can arise in the connectivities between the MTU and the substations.

Table 2. Requirements of Smart Grids vs. anomaly-based approaches

	Complexity	Speed of classification	Speed of learning	Handle parameters	Comprehensibility	Accuracy	Learning from observation	Control - interdep. data	Control - missing data	Control - redundancy	Control - noise	Control - subtle changes	Control - drastic changes	Incremental learning	Unlimited networks	Limited networks	**Requirements**					**Control - Corporative net.**	**Control - RTU/Gateway (Subst.)**	**RTU/Gateway - sensors (Subst.)**	**Gateway - embedded dev. (NAN)**	**Embedded devices (HAN)**
	∓[a]	∓	∓	∓∗	∗	∗	∗	∗	∗	∗	∗	○	○	○			**R1**	**R2**	**R3**	**R4**	**R5**	∗○	∓∗○	∓∗○	○	∓
Classification trees	-	✓	✓	✓	✓	-	-	✗	-	✗	-	-	-	-	✓	●[b]	✓	✗	-	-	-	●	-	-	-	✓
Regression trees	-	-	-	✓	-	-	✓	✗	✓	✗	-	-	-	✓	✓	●	✗	✗	✓	✓	✓	●	-	-	●	-
Association rule learners	✗	-	✓	✗	✓	-	✓	✓	-	✓	✗	-	-	✗	✓	✗	✗	●	✗	✗	✗	●	●	-	-	-
Clustering	✓	✗	✗	✗	✓	✗	✓	✗	✓	✓	✗	-	-	✓	✓	●	●	✗	✓	✓	✓	●	-	-	●	●
Parametric and non-parametric	✓	-	✗	✗	✗	✓	-	-	✓	-	✓	✗	-	-	✓	●	●	✓	●	●	●	✓	✓	●	●	●
Operational models	✓	-	-	✗	✗	✗	-	-	-	-	-	-	✗	-	✓	✓	✓	✗	✗	✗	✗	-	-	-	-	●
Smoothing	✗	-	-	✗	✗	✓		-	✓	-	✓	✓	✗	-	✓	✗	✗	✓	●	●	●	✓	●	-	●	-
Markov chains	✗	-	✗	✗	✗	✓	✓	-	-	-	✗	-	✗	-	✓	✗	✗	✓	✗	✗	✗	●	●	-	-	-
Artificial neural networks	✗	✓	✗	✗	✗	✓	✓	✓	✗	✗	✗	-	-	-	✓	✗	✗	✓	-	-	-	●	●	-	-	-
Bayesian networks	✗	✓	-	✓	✓	-	✓	-	✓	✗	✓	-	-	-	✓	✗	✗	●	-	-	-	●	●	-	-	-
Naïve Bayes networks	-	✓	✓	✓	✓	✗	✓	✗	✓	✗	-	-	-	✓	✓	✗	✓	✗	●	●	●	●	-	-	●	-
Support vector machines	✓	✓	✗	✗	✗	✓	✓	✓	-	✓	✗	-	-	✗	✓	●	✓	●	✗	✗	✗	●	✓	✓	-	●
Rule-based techniques	✓	-	-	✓	✓	✓		-	-	-	✗	-	-	✗	✓	✓	✓	✓	✗	✗	✗	●	✓	✓	-	✓
Rule learners	-	✓	✗	✓	✓	✗	✓	✗	✗	✗	✗	-	-	✗	✓	-	●	✗	✗	✗	✗	●	-	-	-	-
Nearest neighbour	-	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗			✓	✓	-	✗	✗	●	●	●	-	-	-	●	-
Fuzzy logic	✓	✓	✓	✓	✓	✗	-	-	✓	-	✓	-	-	-	✓	✓	✓	✗	-	-	-	●	-	-	-	✓
Genetic algorithm	✗	-	-	✓	-	✗	-	-	-	-	-	-	-	-	✓	✗	✗	✗	✗	✗	✗	-	-	-	-	-
Knowledge-based	✓	-	-	✓	-	✓	-	-	-	-	-	-	-	✓	✓	●	●	✓	●	●	●	✓	✓	●	✓	-
Information-spectral theory	-	-	-	✗	✗	-	-	-	-	✓	✗	✓	-	-	✓	-	✗	✗	-	-	-	●	-	-	-	-

Anomaly-based IDS	✓	✗	✗	✗	✓	✓	✓	●	-	-	-	-
Signature-based IDS	✓	●	-	✓	✗	✗	✗	✓	●	●	●	●
Specification-based IDS	✓	●	-	✓	✓	✓	✓	●	✓	✓	✓	✓

[a] ∓ means that the property complies with [**R1**]; ∗ with [**R2**]; and ○ with [**R3, R4, R5**].

[b] ● states the benefits for the network device but with 'dependence' on the functional features of the approach (e.g., data structure, abilities to control noise, changes, etc.) regarding the hardware or software constraints.

- **Support vector machines**: this method is powerful and well-suited to dealing with large numbers of features. SVMs are accurate ([**R2**]) and they have low complexity models ([**R1**]) [2]. However they present problems in the speed of the learning process, a handicap that makes SVMs difficult to implement in networks with constrained resources, and particularly in the presence of dynamic scenarios. Nevertheless, this can be easily overcome in networks with sufficiently powerful nodes (e.g., gateways) deployed in rather static scenarios, where the set of representative training instances is small.
- **Statistics**: optimized parametric or non-parametric solutions can become effective approaches for these sections of the Smart Grid, but without considering those related to operational models, since these do not guarantee the fulfilment with [**R2**].

In addition, the detection methods that have problems in addressing overfitting do not have as big an impact as the corporate networks, because the stability and periodicity of the scenario makes the classification instances very similar to the training datasets. However, signature-based IDSes configured inside RTUs can become complex since these IDSes requires big databases with known threat patterns to be kept, forcing the RTU to depend on external databases. However, **specification-based** IDS could be a good candidate since legitimate specifications of the interfaces are well known, and sometimes limited in terms of specification, favouring the definition of threat patterns according to the technical characteristics of the devices. This criteria is also applicable for constrained devices such as sensors or smart meters [19].

Another important part of a substation is the communication between RTU/ gateways working in ISA100.11a/ WirelessHART (or coordinators in ZigBee) and the industrial sensor nodes. These sensors are heavy-duty devices with restrictions on executing complex operations and algorithms, and these generally maintain a regular and static traffic where their functions consist of constantly monitoring an object or an infrastructure, and sending this information to the gateway. Assuming that the communications are completely synchronous, our goal is now to find those lightweight solutions that ensure, at least, [**R1, R2**]; and in this way, do not degrade the operational activities in the field, such as:

- **Rule-based** techniques: this method, described above, is a simple approach that can be computed by constrained devices, but its effectiveness will depend on how the rules and threat scenarios are defined.
- **Support vector machines**: SVM methods, as we discussed, have good qualities to be used as detection engines for the IDSes deployed in constrained networks (favouring [**R1, R2**]). But to apply the method, it is necessary that these networks need to ensure regular and static traffic patterns to avoid triggering the learning processes with frequency.
- Optimized **statistic-based** solutions: as mentioned, these can also become quite effective for [**R1, R2**], since their approaches present a moderate complexity and a high efficiency. However, the feasibility also depends on the optimization degree to avoid overhead costs.

The communication between industrial sensors is thoroughly analysed in the next section because home appliances and smart meters present similar behaviours.

4.3 Neighbourhood and House Areas: Metering and Control

The type of data managed in the hierarchical communications (NANs) between data aggregation point and metering devices (smart meters) and its relation to the end-users, makes the topics related to security and privacy prevail over questions of control; but this control must exist as well. Depending on the characteristics of the interfaces and assuming a constant communication, **knowledge-based** approaches can be good candidates to ensure [**R3, R4, R5**] together with those related to the **statistics** (e.g., smoothing approaches). As regards HAN networks, the communication between embedded devices ((weak, normal or heavy-duty) sensors, smart meters and home appliances) becomes the most predominant infrastructure for the constant monitoring and reporting of consumption evidence to smart meters. Their efficiency, however, depends on the type of energy consumption of these activities (many of these devices are very dependent on batteries), software and hardware capabilities, and even, on the type of configuration of their networks, overwhelmingly ad-hoc in nature. Therefore, the selection of techniques should primarily be focused on complying with [**R1**], such as:

- **Decision trees**, **Fuzzy logic**, **rule-based** techniques: these three approaches are in general fast and efficient learners and classifiers ([**R1**]); a set of functional features for those application scenarios built on strong restrictions and constrained devices [18]. Nonetheless, we could also consider the **operational models** for their simplicity, but always keeping in mind the need to define appropriate normality thresholds.
- Optimized **statistic** and **clustering** techniques: a well-configured simple approaches could result in a lightweight detection tool ([**R1**]). In the case of clustering, this solution would be more valid and useful in a scenario where the patterns of behaviour suffer few variations, and the learning and testing mechanisms are seldom triggered.

On the other hand, ad-hoc networks could be used by human operators for local control, acquisition and management of controllers, sensors, actuators, smart meters and other related devices for control. In this regard, the control establishes a collaborative environment where human operators can directly operate in the field or in populated areas (e.g., to locally check neighbourhood areas, status values of energy charging spots) without going through the control centre; thereby facilitating the execution of actions in real-time and the mobility within the area. This collaboration is generally based on very diverse kinds of technologies (e.g., PDA, cellular devices) with similar capacities to the technical specifications defined for the heavy-duty devices in Sect. 2, and hence, they can adopt similar approaches to those described for sensors. But due to their relativity to control ([**R2, R3, R4**]), their lightweight IDS solutions should also consider supplementary mechanisms, such as secure aggregation and reputation methods, to provide extra layer of protection and improve the detection procedures in the face of sophisticated threats. At this point, we also conclude that methods with costly training processes are less appropriate for dynamic networks regardless of the computational power of their nodes. This is because the constant changes and new dynamics constantly appearing in those networks make the IDSes trigger the learning mechanisms more frequently, and in this case they are computationally costly. However, in networks with regular and constant traffic, the training procedures are triggered only a few times, thus the use of these methods does not produce overhead excess in the system.

5 Conclusions

A set of anomaly-based techniques have been analysed in this paper so as to explore and exploit functionalities for context-awareness in Smart Grid environments. The result is a comparative study in the form of a guideline that helps in the selection of most suitable schemes and detection modes according to the restrictions of the context and functional characteristics of the technologies and communication systems (see Table 2). Taking into account this guideline, our future work will consist of investigating lightweight solutions that aim to detect stealth attacks in the different control domains that comprise a Smart Grid.

Acknowledgment. The results of this research have received funding from the Marie-Curie COFUND programme U-Mobility, co-financed by the University of Málaga, the EC FP7 under GA No. 246550 and the Ministerio de Economía y Competitividad (COFUND2013-40259). The second author has been funded by a FPI fellowship from the Junta de Andalucía through the project FISICCO (P11-TIC-07223). Additionally, this work has been partially supported by the research project ARES (CSD2007-00004) and the EU FP7 project FACIES (HOME/2011/CIPS/AG/4000002115).

References

1. Chandola, V., Banerjee, A., Kumar, V.: Anomaly detection: a survey. ACM Comput. Surv. **41**(3), 15–58 (2009). 15
2. Kotsiantis, S., Zaharakis, I., Pintelas, P.: Supervised machine learning: a review of classification techniques. In: Frontiers in Artificial Intelligence and Applications, pp. 249–268 (2007)
3. Gyanchandani, M., Rana, J., Yadav, R.: Taxonomy of anomaly based intrusion detection system: a review. Neural Netw. **2**(43), 1–14 (2012)
4. Yan, Y., Qian, Y., Sharif, H., Tipper, D.: A survey on smart grid communication infrastructures: motivations, requirements and challenges. IEEE Commun. Surv. Tutor. **15**(1), 5–20 (2013)
5. Roman, R., Alcaraz, C., Lopez, J.: A survey of cryptographic primitives and implementations for hardware-constrained sensor network nodes. Mob. Netw. Appl. **12**(4), 231–244 (2007)
6. Abowd, G.D., Dey, A.K.: Towards a better understanding of context and context-awareness. In: Gellersen, H.-W. (ed.) HUC 1999. LNCS, vol. 1707, p. 304. Springer, Heidelberg (1999)
7. Alcaraz, C., Lopez, J.: Wide-area situational awareness for critical infrastructure protection. IEEE Comput. **46**(4), 30–37 (2013). IEEE Computer Society
8. Bhuyan, M., Bhattacharyya, D., Kalita, J.: Network anomaly detection: methods, systems and tools. IEEE Commun. Surv. Tutor. **99**, 1–34 (2013)
9. Fan, J.: Nonlinear Time Series: Non-parametric And Parametric Methods. Springer, Handbook (2003)
10. Demand Planning, Exponential Smoothing (SCM-APO-FCS), SAP. http://help.sap.com/. Accessed May 2014
11. Friedman, N., Geiger, D., Goldszmidt, M.: Bayesian network classifiers. Mach. Learn. **29**(2–3), 131–163 (1997)

12. Jyothsna, V., Prasad, R.V.V.: A review of anomaly based intrusion detection systems. Int. J. Comput. Appl. **28**(7), 26–35 (2011)
13. Shanmugam, B., Idris, N.: Hybrid intrusion detection systems (HIDS) using Fuzzy logic. In: Skrobanek, P. (ed.) Intrusion Detection Systems, pp. 135–155, Chap. 8. InTech (2011)
14. Mackay, D.: Information Theory, Inference and Learning Algorithms. Cambridge University Press, Cambridge (2003)
15. Cazorla, L., Alcaraz, C., Lopez, J.: Towards automatic critical infrastructure protection through machine learning. In: Luiijf, E., Hartel, P. (eds.) CRITIS 2013. LNCS, vol. 8328, pp. 197–203. Springer, Heidelberg (2013)
16. Chow, M., Yee, S., Taylor, L.: Recognizing animal-caused faults in power distribution systems using artificial neural networks. IEEE Trans. Power Delivery **8**(3), 1268–1274 (1993)
17. Choi, K., Chen, X., Li, S., Kim, M., Chae, K., Na, J.: Intrusion detection of NSM based DoS attacks using data mining in Smart Grid. Energies **5**, 4091–4109 (2012)
18. Kher, S., Nutt, V., Dasgupta, D., Ali, H., Mixon, P.: A detection model for anomalies in smart grid with sensor network. In: Future Instrumentation International Workshop (FIIW), pp. 1–4 (2012)
19. Jokar, P.: Model-based intrusion detection for Home Area Networks in Smart Grids, pp. 1–19. University of Bristol, Bristol (2012)
20. Najy, W., Zeineldin, H., Alaboudy, A., Woon, W.: A bayesian passive islanding detection method for inverter-based distributed generation using ESPRIT. IEEE Trans. Power Delivery **26**, 2687–2696 (2011)
21. Shahid, N., Aleem, S., Naqvi, I., Zaffar, N.: Support vector machine based fault detection & classification in smart grids, pp. 1526–1531. Globecom, IEEE (2012)
22. Zhang, Y., Wang, L., Sun, W., Green, R., Alam, M.: Distributed intrusion detection system in a multi-layer network architecture of smart grids. IEEE Trans. Smart Grid **2**(4), 796–808 (2011)
23. Mitchell, R., Chen, I.R.: Behavior rule based intrusion detection systems for safety critical smart grid applications. IEEE Trans. Smart Grid **4**, 1254–1263 (2013)
24. Sedghi, H., Jonckheere, E.: Statistical structure learning: towards a tobust Smart Grid, arXiv, pp. 1–16 (2014)
25. Chan, S., Tsui, K., Wu, H., Hou, Y., Wu, Y., Wu, F.: Load/price forescasting and managing demand response for smart grids. IEEE Signal Process. Mag. **29**, 68–85 (2012)
26. Chang, C., Wang, Z., Yang, F., Tan, W.: Hierarchical fuzzy logic system for implementing maintenance schedules of offshore power systems. IEEE Trans. Smart Grid **3**(1), 3–11 (2012)
27. Manjili, Y., Rajaee, A., Jamshidi, M., Kelley, B.: Fuzzy control of electricity storage unit for energy management of Micro-Grids. In: World Automation Congress, pp. 1–6. IEEE (2012)
28. Calderaro, V., Piccolo, A., Siano, P.: Failure identification in smart grids based on petri net modeling. IEEE Trans. Industr. Electron. **58**(10), 4613–4623 (2011)
29. Syafaruddin, S., Karatepe, E., Hiyama, T.: Controlling of artificial neural network for fault diagnosis of photovoltaic array. In: The 16th International Conference on Intelligent System Application to Power Systems, pp. 1–6. IEEE (2011)
30. Chien, C., Chen, S., Lin, Y.: Using bayesian network for fault location on distribution feeder. IEEE Trans. Power Del. **17**(3), 785–793 (2002)
31. Samantaray, S., El-Arroudi, K., Joos, G., Kamwa, I.: A Fuzzy rule-based approach for islanding detection in distributed generation. IEEE Trans. Power Delivery **25**(3), 1427–1433 (2010)

Springer

http://www.springer.com/978-3-319-17126-5

Risks and Security of Internet and Systems
9th International Conference, CRiSIS 2014, Trento, Italy,
August 27-29, 2014, Revised Selected Papers
Lopez, J.; Ray, I.; Crispo, B. (Eds.)
2015, XI, 275 p. 70 illus., Softcover
ISBN: 978-3-319-17126-5