Learning from Loads: An Intelligent System for Decision Support in Identifying Nodal Load Disturbances of Cyber-Attacks in Smart Power Systems Using Gaussian Processes and Fuzzy Inference

Miltiadis Alamaniotis and Lefteri H. Tsoukalas

Abstract The future of electric power is associated with the use of information technologies. The smart grid of the future will utilize communications and big data to regulate power flow, shape demand with a plethora of pieces of information and ensure reliability at all times. However, the extensive use of information technologies in the power system may also form a Trojan horse for cyberattacks. Smart power systems where information is utilized to predict load demand at the nodal level are of interest in this work. Control of power grid nodes may consist of an important tool in cyberattackers' hands to bring chaos in the electric power system. An intelligent system is proposed for analyzing loads at the nodal level in order to detect whether a cyberattack has occurred in the node. The proposed system integrates computational intelligence with kernel modeled Gaussian processes and fuzzy logic. The overall goal of the intelligent system is to provide a degree of possibility as to whether the load demand is legitimate or it has been manipulated in a way that is a threat to the safety of the node and that of the grid in general. The proposed system is tested with real-world data.

1 Introduction

The application of digital control system technologies and sensor networks for monitoring purposes in critical power facilities is a topic of high interest [1]. The use of digital technologies offers significant advantages that include reduction in the purchase and maintenance costs of facility components and equipment, and a significant reduction in the volume of hardware deployed throughout the facility [2].

M. Alamaniotis (✉) • L.H. Tsoukalas
Applied Intelligent Systems Laboratory, School of Nuclear Engineering,
Purdue University, West Lafayette, IN, USA
e-mail: malamani@ecn.purdue.edu; tsoukala@ecn.purdue.edu

I. Palomares et al. (eds.), *Data Analytics and Decision Support for Cybersecurity*,
Data Analytics, DOI 10.1007/978-3-319-59439-2_8

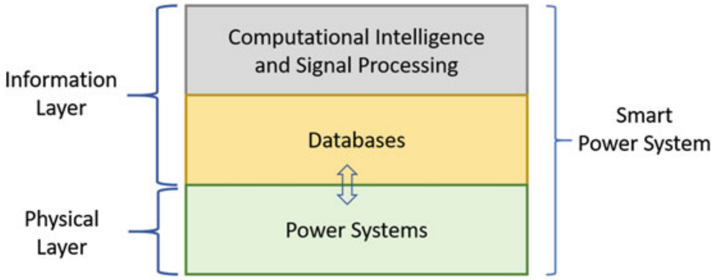

Fig. 1 The notion of smart power systems that are comprised of two layers

The basic mission of power systems is the nonstop delivery of generated electricity to connected consumers. Delivery systems have been equipped with several monitoring, prognostics and diagnostics tools, as well as several redundant systems and mechanisms [3]. It should be noted that redundancy refers to availability of more than required systems and mechanisms that perform the same operation. Redundancy allows retaining of the normal operation of the power system in case a system or mechanism fails, given that the rest will compensate for it. Thus, power systems exhibit high resiliency and fault tolerance behavior in fulfilling their mission of 24/7 power delivery. The advent of computers and internet connectivity added one more factor that should be taken intro serious consideration: cyber security [4]. The advantages offered by the ever increasing use of computer and communication technologies (ICT) in power system operation, come at a cost of new vulnerabilities in system security. What was formerly a physically isolated system is now open to unauthorized access and manipulation control through potential vulnerabilities posed by ICT use [5]. For instance, the supervisory control and data acquisition (SCADA) systems consist of the backbone of the overall power system monitoring and subsequent decision-making processes. Hence, despite their nowadays practical benefits, SCADA systems present serious targets for cyber-attackers.

The advent of smart power technologies is expected to couple data technologies with conventional power systems in ways that optimizes energy consumption and minimizes loses [6]. The notion of smart power systems is visualized in Fig. 1, where it can be observed that the smart power system is a form of a cyber-physical system [7, 8]. The information (i.e., cyber) layer is comprised of two modules. The first module includes the intelligent systems and signal processing tools and the second module the databases. Those two modules are complementary; the intelligent tools utilized stored information to make management decisions pertained to power system operation [9]. The second layer is the physical layer that contains the physical components of the power system.

Given that smart power systems are heavily dependent on data and information processing tools as it is depicted in Fig. 1, cybersecurity is a major issue that cannot be overlooked. Every asset of smart power systems may be compromised and subsequently be transformed into a vehicle for conducting a cyber-attack [10].

In contrast to physical attacks, the nature of cyber-attacks imposes significant difficulties in detecting, isolating and mitigating the consequences of cyber-attacks. Additionally, estimation of a cyber-attack impact is a difficult task given that full detection of all parts that have been affected by the attack, if possible, may take a significant amount of time [11]. Full recovery is also a time-consuming process. The cyber-attack in Ukrainian power grid on December 2015 presents an example in which computer control is not fully restored yet [12, 13]. In addition, cyberattacks may be used as a proxy for a subsequent physical attack in critical energy facilities. For instance, manipulation of digital access may allow a person to get access to areas of nuclear material disposal that may be used for nefarious purposes [14].

Detection of cyber-attacks and their consequences in operation of smart power systems may be characterized as a multi-stage task. This is true since these systems contain the physical layer (power infrastructure) as well as the cyber layer (information technologies) [15–17]. Furthermore, the correlations among the two layers as well as the associations between components of the same layer makes detection of the source of an attack a very challenging task. For example, a cyber-attack's objective may be to cause a disturbance in a substation and thus it attempts to take control over the smart relays that reside in that substation [18, 19]. Hacking the operator's computer may perform this type of attack, that is, stealing its login credentials, and then through the operators' computer and substation communication, the hacker assumes control of the protective relays [20].

The technological success and prevalence of smart power technologies may facilitate the development of intelligent scientific methods and tools for achieving effective grid cybersecurity from various perspectives. To that end, research efforts will contribute in detecting cyberattacks utilizing power consumption and forecasting information [21]. Intelligent monitoring tools may be connected to a node of the power grid infrastructure and independently of the wide area monitoring system (WAMS) obtain and process node data [22]. Hence, nodal analysis of power information may reveal discrepancies between expected and actual consumption at that node.

In this work, we study the suitability of load demand information, and we present "learning from loads" as a method for detecting disturbances in power systems nodes. In particular, we introduce an intelligent system as a means for detecting load disturbances at the nodal level. We theorize that an intelligent system will leverage the non-linear dynamics of the load demand of a very short term horizon, and that will be adequate to distinguish malicious disturbances from normal ones. Load demand at the nodal level results from the aggregation of individual consumer demands. Individual demand exhibits high variance while the aggregation of multiple demands provides a signal that is smoother. In simple terms we can say that the greater the number of individual consumers or nodes, the higher the smoothing of the demand signal. Thus, aggregation poses difficulties in identifying load disturbances because aggregation may mask the disturbances on a single individual node. In our work, we implement an intelligent system that utilizes the synergism of Gaussian process regression (GPR) and fuzzy logic. The GPR is used for prediction while the fuzzy logic tool makes inferences regarding decisions as to whether the demand is legitimate or it has been manipulated by an attacker.

The remainder of this chapter contains five sections. Section 2 briefly introduces GPR and fuzzy logic inference, while Sect. 3 introduces smart power system and in particular Energy internet. Section 4 describes the proposed intelligent system. Section 5 presents the results obtained by applying the intelligent system to a set of load demand data. At the end, Sect. 6 concludes and summarizes the salient points of our approach.

2 Background

This section is dedicated in briefly presenting the theoretical foundation underlying our approach. In particular, the Gaussian Process Regression in the context of kernel machines will be introduced followed by a short discussion on fuzzy logic inference. The theory presented in this section will foster the ground for understanding the proposed intelligent system.

2.1 Gaussian Process Regression

Machine learning has been identified as one of the pillars in developing efficient data analytics methods and decision support systems. One of the preeminent areas of machine learning is the class of non-parametric methods called *kernel machines*.

A kernel machine is any analytical model that is a function of a kernel [23]. A kernel (a.k.a., *kernel function*) is any valid analytical function that takes the following form:

$$k\,(x_1, x_2) = \varphi(x_1)^T \cdot \varphi\,(x_2) \tag{1}$$

where, $\varphi(x)$ is called the basis function, and x_1, x_2 are input values. The inputs to a kernel may be either both scalar or vector values of equal length. Their range of values depends on the problem under study, while the kernel output represents the similarity between the input values. In general, selection of the basis function falls within responsibilities of the modeler and depends on the specifics of the application at hand [24]. For instance, the simplest basis function is $\varphi(x) = x$ and therefore the respective kernel takes the form given below:

$$k\,(x_1, x_2) = {x_1}^T \cdot x_2 \tag{2}$$

which is simply known as the linear kernel. It should be noted that formulation of models using kernels whose form can be determined by the modeler is called the *kernel trick* and finds wide use in data analytics and pattern recognition applications [23].

The class of kernel machines contains the Gaussian processes (GP). Gaussian processes may be modeled as a function of a kernel. In particular, the kernel enters into the Gaussian process formulation through its covariance function. A kernel-modeled Gaussian process can be used either in classification or regression problems. In the latter case, it is identified as Gaussian process regression [23].

Likewise Gaussian distribution, a Gaussian process is identified via its two parameters, namely, the mean function and the covariance function denoted by m(x) and C(x^{T},x) respectively. Thus, we get [23]:

$$GP \sim N\left(m(x), C\left(x^T, x\right)\right). \tag{3}$$

Derivation of the GPR framework has as a starting point Eq. (3) where we set

$$m(x) = 0, \tag{4}$$

and

$$C\left(x^T, x\right) = k\left(x^T, x\right). \tag{5}$$

Selection of *m(x)=0* is a convenient choice, while the covariance function is replaced by a kernel function [23]. In that way, GPR is transformed into a kernel machine that may be used in regression problems.

The above GPR formulation necessitates the availability of datasets, i.e., known targets **t** for known inputs **x** (in other words training datasets). The size of the training population is denoted as *N*. Thus, we assume that we have *N* known data points, which are consolidated in a matrix $\mathbf{x}_N$, and we denote a new unknown one as x_{N+1}. The respective target associated with x_{N+1} is denoted as $t_{\mathrm{N}+1}$. It should be noted that GPR considers the joint distribution between the *N* training data points and the unknown x_{N+1} to be s a Gaussian distribution. Based on that assumption, it has been shown in [25, 26] that GPR provides a prediction interval over the target $t_{\mathrm{N}+1}$ that is denoted in the form of a predictive distribution. That predictive distribution is Gaussian with a mean and covariance function given by:

$$m\left(x_{N+1}\right) = \mathbf{k}^T \mathbf{C}_N^{-1} \mathbf{t}_N \tag{6}$$

$$\sigma^2\left(x_{N+1}\right) = k - \mathbf{k}^T \mathbf{C}_N^{-1} \mathbf{k} \tag{7}$$

with $\boldsymbol{C}_{\mathrm{N}}$ being the covariance matrix among the *N* training data, $\boldsymbol{k}$ being a vector of covariances between the input x_{N+1} and the *N* training data, and *k* the scalar value taken as $k(x_{\mathrm{N}+1}, x_{\mathrm{N}+1})$ [23].

Thus, kernel selection should be done carefully and with respect to the respective GPR output. Overall, kernel-based GPR offers flexibility in prediction-making; the modeler is able to select a kernel among existing ones or compose a new kernel. Hence, the kernel form can be tailored to the specifics of the prediction problem, allowing the modeler to have flexibility in the way he builds his prediction model.

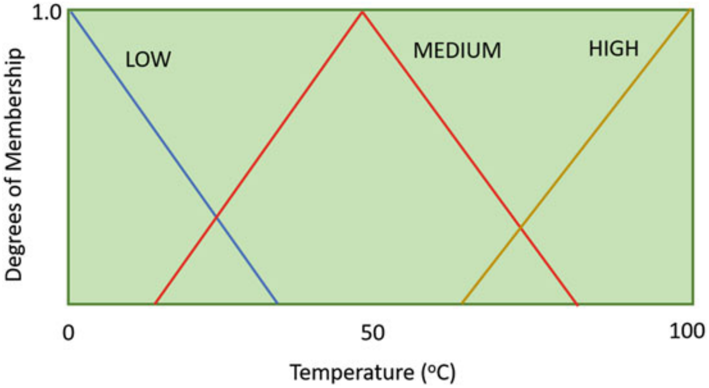

Fig. 2 Example of fuzzy sets pertained to temperatures [0, 100] °C

2.2 Fuzzy Logic Inference

Fuzzy logic is a branch of artificial intelligence that finds application in data analytics under vagueness. The strength of fuzzy logic is the representation of vaguely expressed knowledge via the use of linguistic descriptions. Each linguistic description is modeled by a fuzzy set [27], which may be seen as an extension of the classical set theory.

In classical set theory, an object clearly belongs to a set or not. In other words, crisp sets follow a digital logic, where an object either belongs to a set and take a value 1 for that set, or does not and takes a value of 0. A fuzzy set defined over a universe of discourse U is a set whose objects in U belong to the set up to a degree; the degree values are taken in the interval [0 1]. For instance, an object may belong to a set *A* with a degree of membership equal to 0.3 while at the same time it belongs to the set *B* with a degree of membership equal to 0.8. It should be noted that crisp sets may be seed as fuzzy sets whose objects take degrees of membership either 1 or 0.

Evaluation of the degrees of membership is performed via the use of the membership function. A membership function assigns to each object of the universe of discourse a number in the interval [0 1] that denotes the degree to which this object belongs to the set. Figure 2 shows an example where the temperatures [0, 100] °C are spanned by three fuzzy sets.

The use of fuzzy sets facilitates implementation of fuzzy inference mechanisms called fuzzy inference. The fuzzy inference mechanism is expressed via the use of *IF..THEN* rules, where the *IF* part contains the conditions, and the *THEN* part contains the consequences. For instance, two simple rules may have the following form:

$$IF\ x\ is\ A, THEN\ y\ is\ B$$

$$IF\ x\ is\ C, THEN\ y\ is\ D$$

where *A*, *B*, *C* and *D* are fuzzy sets. By using the sets in Fig. 2, an example of a fuzzy controller for a heating system might have the following rules:

$$\textit{IF temperature is LOW},\ \textit{THEN heater intensity is HIGH}$$

$$\textit{IF temperature is MEDIUM},\ \textit{THEN heater intensity is MEDIUM}$$

$$\textit{IF temperature is HIGH},\ \textit{THEN heater intensity is LOW}$$

where, *temperature*, and *heater intensity* are called fuzzy variables.

Overall, a fuzzy inference system is comprised of several rules of the above form. In fuzzy inference systems one or more rules may be fired and therefore a fuzzy output is taken [28]. In that case, a defuzzifying step is utilized to obtain a single output value [27, 28]. One of the widest used methods of defuzzification is the *center of area* (COA) method whose analytical formula is given below [27]:

$$y^* = \frac{\sum_{n=1}^{N} x_n \mu_A(x_n)}{\sum_{n=1}^{N} \mu_A(x_n)} \tag{8}$$

where $y*$ is the defuzzified output value, and $\mu_A(x_n)$ is the degrees of membership of the input x_n to fuzzy set A. The COA may be seen as the weighted average value of the obtained fuzzy output; in practice it computes the area below the fuzzy output and finds its mean value.

Fuzzy inference has found various applications and fuzzy systems for developing decision support systems are under development. The interested reader is advised to check Ref. [27] for details on fuzzy inference, where several illustrative examples are described in detail.

3 Smart Power Systems: The Energy Internet Case

This section includes a short introduction of the concept of price-directed smart power systems and in particular the principle idea of an Energy Internet as proposed by the Consortium for the Intelligent Management of Electric Grid (CIMEG) [28]. The goal of this section is to provide the general framework of smart power systems and show the general environment in which the proposed intelligent system is of practical use.

The Energy Internet exploits advancements of information networks to leverage energy utilization. Crucial in implementing an Energy Internet are energy anticipation at consumer and at nodal level, smart meter negotiations, and determination of real-time price signaling [30]. The general block diagram of a smart power system developed by CIMEG is presented in Fig. 3. CIMEG models the power grid as a demand-driven system. It adopts a bottom up approach to determine the global state of grid health. To that end, CIMEG introduced the notion of a Local Area Grid

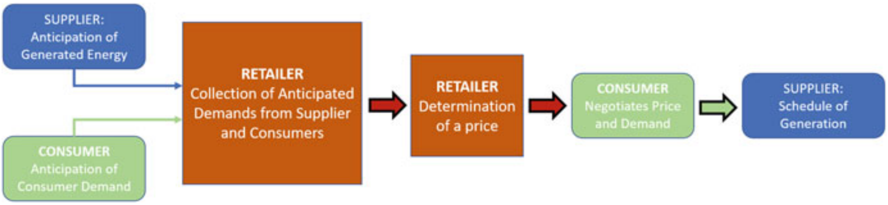

Fig. 3 General framework of Smart Power Systems implemented as an Energy Internet [30]

(LAG) that is characterized as the clustering of several different consumers. A LAG is responsible for keeping its own stability by taking the necessary actions when appropriate [6].

We observe in Fig. 3 that the individual consumers provide an anticipation of their demand for a specific ahead of time horizon. At the same time, suppliers also anticipate their generated electrical energy for the same time horizon. Both parties, i.e., consumers and suppliers forward their anticipated signals to the retailers. Subsequently, the retailer collects the anticipations and by utilizing price elasticity models determines a price for each of the consumer. Then, the consumer has the opportunity to negotiate the price with the retailer by altering its initial anticipated demand [31]. Through negotiations, retailer and consumer come to an agreement. Once all consumers make an agreement with the retailer, then the generator schedules the generated energy to meet final demand.

Iteration of the above process may take place at every system operational cycle. Details on smart power and Energy Internet may be found in references [6, 32, 33].

4 "Learning From Loads" Intelligent System

Having introduced the framework of smart power (energy internet) this section presents the "learning from loads" system to detecting nodal load disturbances for enhancing cybersecurity in this framework. In the following subsection, the proposed methodology as well as the attack scenarios pertained to load disturbances are presented.

4.1 Intelligent System Architecture

In this section, the intelligent system that makes decisions pertained to nodal load with respect to cybersecurity is presented. It should be noted that the proposed intelligent system exploits current as well as future information via the use of anticipation functions. Anticipation will allow the system to evaluate its future states compared to what it has seen so up to this point. To that end, a learning from load demand approach is adopted, and subsequently anticipates the future demand.

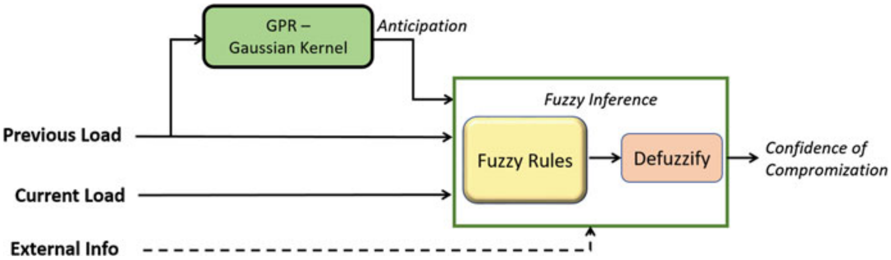

Fig. 4 Block diagram of the proposed learning from loads intelligent system

Anticipation is utilized to evaluate the actual demand and make inferences whether data have been manipulated or not.

The block diagram of the proposed system is depicted in Fig. 4. We observe that there are two paths. The first path analyzes recorded data and anticipates future load, while the second path utilizes the current load. In addition, to the above paths, we may observe in Fig. 3 that there is a subsidiary path that contains external information pertained to that specific node. For instance, the price of electricity at current time.

Load anticipation is performed using kernel modeled Gaussian process regression, which was introduced in the previous section. The GPR is equipped with a Gaussian kernel whose analytical form is given below:

$$k\left(x_1, x_2\right) = \exp\left(-\frac{\|x_1 - x_2\|^2}{2\sigma^2}\right) \tag{9}$$

where σ^2 is a kernel parameter whose value is being determined in the training phase of the algorithm. The GPR model is trained on previous recorded load demands. Once the training is finished the GPR is utilized for making prediction of the future demand. Therefore, we observe that this is the first point at which our system learns from loads (i.e., past loads).

Further, we observe in Fig. 3 that the information, anticipated, previous and current loads are fed to a fuzzy inference system [34]. In addition, the external information is also directly fed to the fuzzy inference system. Overall, it should be noted that the available information is forwarded to the fuzzy inference.

The fuzzy inference system is comprised of two parts as Fig. 3 depicts. The first part contains the fuzzy rules utilized for making inference. The fuzzy rules are predetermined by the system modeler and they take the form of IF.. THEN rules as shown in Sect. 2 as well. The left-hand side of the rules, i.e., conditions, may be refer to anticipated load or current load. In particular, the rules for anticipated load have the following general form:

$$\textit{IF Future Load will be } A_F(t), \textit{ THEN Confidence of Compromise is } B(t)$$

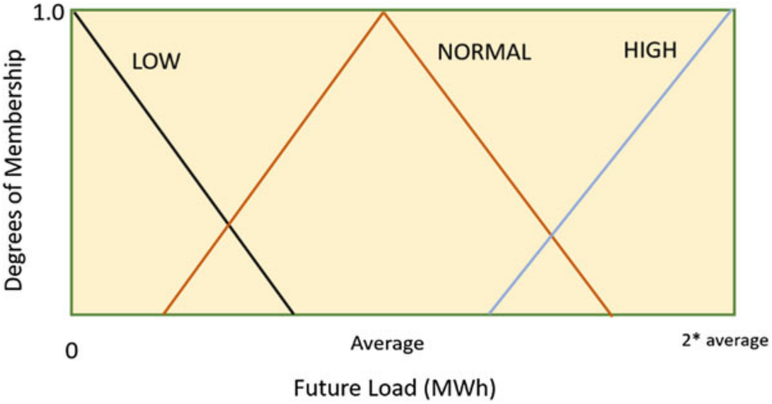

Fig. 5 Fuzzy sets for fuzzy variable *Future Load*

where the fuzzy variable is *Future Load* and A_F denotes the fuzzy values (see Fig. 5) while the rules for current load have the form:

$$IF\ Current\ Load\ is\ A(t),\ THEN\ Confidence\ of\ Compromise\ is\ B(t).$$

with Current Load being the fuzzy variable in that case (see Fig. 6).

In addition, we defined a new fuzzy variable which is equal to the absolute difference between the Anticipated Load and the Actual Load of the same time interval, i.e.:

$$Difference = |\ Anticipated\ Load\text{–}\ Actual\ Load\ |$$

where the variable Difference is actually the fuzzified value obtained by subtraction of anticipated and actual load. This fuzzy variable will allow to measure how much was the inconsistency between the anticipated and the actual load over the same time interval. It should be noted that the actual load is different from the current load. The current load exhibits the current load demand while the actual load variable refers to the actual demand for the time interval that the anticipation was made. This is a fundamental inference variable given that the offset between anticipation and actual may “reveal” the presence of a threat or not.

Lastly, we model the current prices of electricity as external information. The presented intelligent system aspires to be deployed in smart power environment (energy internet) and therefore price will play an important role in justifying load disturbances. The price will show the willingness of the consumer to change its consumption. For instance, an attacker will increase the load demand no matter how high the prices are; that can be used as an indicator to identify potential attackers. The rules pertained to price have the following form:

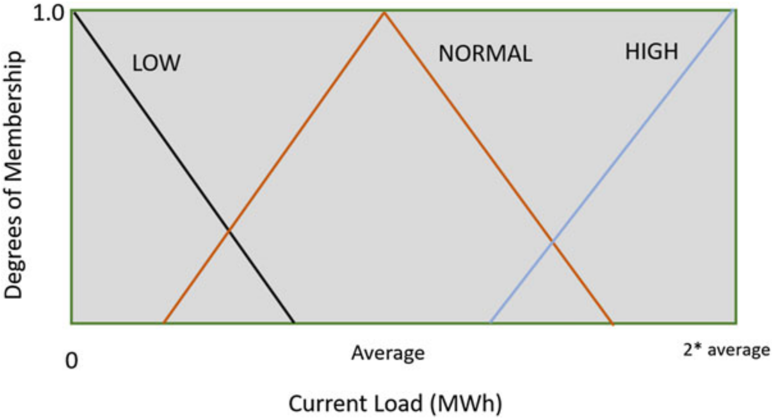

Fig. 6 Fuzzy sets for fuzzy variable *Current Load*

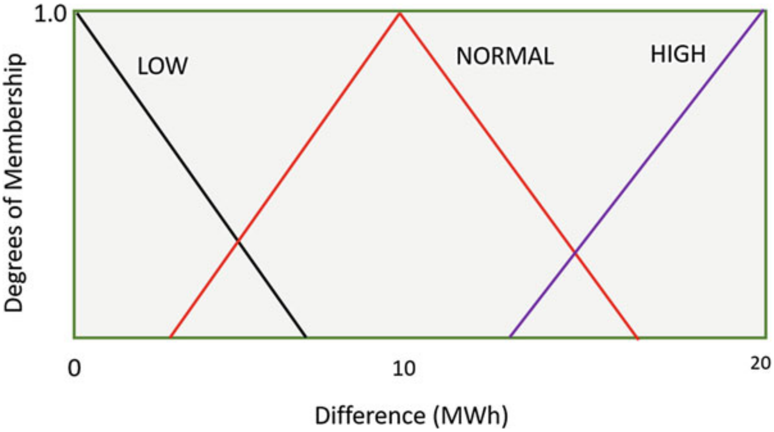

Fig. 7 Fuzzy sets for fuzzy variable *Difference*

$$IF\ Price\ is\ A(t),\ THEN\ Confidence\ of\ Compromise\ is\ C(t).$$

Additionally, it should be noted that as an external information we consider: (1) the average current load that we observe for that node, and (2) the average anticipated load that the GPR provides. These values may be found by keeping record of previous values.

Figures 5, 6, 7, and 8 provide the fuzzy sets of the fuzzy variables *Future Load*, *Current Load*, *Difference,* and *Price* respectively, while Fig. 9 depicts the fuzzy sets of the *Confidence of Compromise* variable (the confidence scale is in interval [0 1]). The fuzzy inference overall was comprised of 20 fuzzy rules and was implemented in Matlab software.

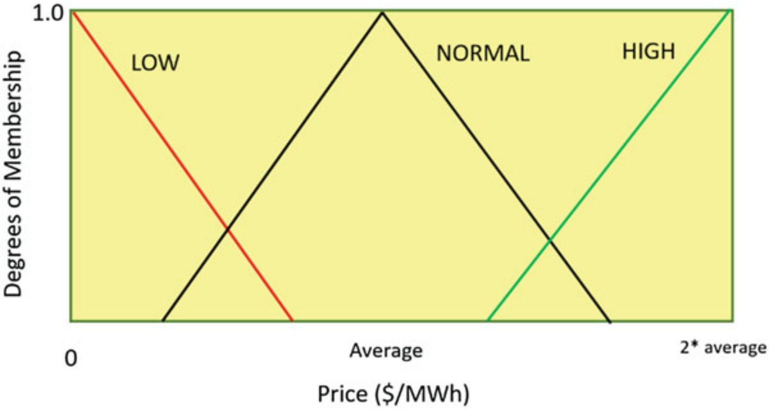

Fig. 8 Fuzzy sets for fuzzy variable *Price*

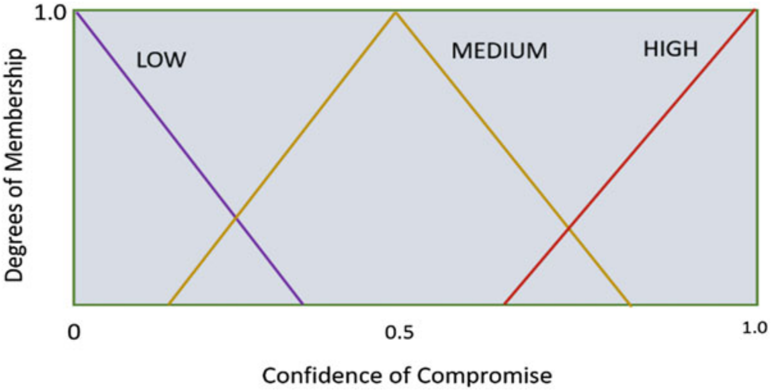

Fig. 9 Fuzzy sets for fuzzy variable *Current Load*

The second part of the fuzzy inference systems includes the defuzzification part. The defuzzification uses the center of area method [27] whose form is given in Eq. (8). The defuzzification provides a crisp output that is also the final output of the system. The output value is the confidence of compromise pertained to load disturbances for that node. The value of the confidence may support the power system operators and security engineers to make decisions whether there is cyber-attack pertained to load demand.

4.2 Type of Threats for Nodes of Smart Power Systems

The experience of cyberattack in the Ukrainian power system in December 2015, proved that the tactical preparation of the cyber-attackers maybe well defined and planned over a long time. Furthermore, the attackers may show patience, perform long term reconnaissance and follow a carefully planned series of actions. Given that smart power systems are heavily dependent on the utilization of information, the cyberattacks may also involve a significant deal of grid congestion by increasing nodal load demand.

The scenario that we examine in this work is the following:

- A cyberattacker wants to cause a blackout in a part of the grid. One way to achieve this is by destabilizing one of the grid nodes. Destabilzation can be done by increasing the demand beyond the capacity limits of the node. Therefore, the node will become nonoperational and the power delivery will fail at that point. In addition, if that node is at the backbone of the grid then it may propagate the problem to the rest of the grid.
- A simple way to cause this type of attack is to compromise the intelligent meters of several consumers that are connected to that node. As we noted, in the vision of Energy Internet the consumer negotiates with the retailer. Negotiations may be undertaken by the attacker with the consumer having no knowledge about it. Overall, by taking into control several of the consumers the attacker may cause a blackout in the node.

In the next section, the above scenario will be employed in a real case scenario. Nodal demand from real-world datasets will be used as our test scenario. The intelligent system will be utilized to analyze the load (current and anticipated) and output a confidence value whether there is manipulated increase in load demand.

5 Results

In this section, we test the proposed intelligent system on a set of real world data. The datasets contain the hourly values of loads and energy prices within the smart grid system, for one day before the targeted day. For visualization purposes the actual demand signal is given in Fig. 10.

The goal is detect whether the security status of a node in the grid was compromised. We assume that load demands are recorded every hour. Therefore, the GPR model is utilize for anticipating the load for the next hour. The predicted signal is depicted in Fig. 11. It should be noted that the training of the GPR was performed by utilizing the demand data of one and two days before the targeted day.

In our work, we tested our intelligent system on the following scenarios:

(1) No compromise has occurred.
(2) From 12.00 pm to 15.00 pm, the node is compromised and 10% increase in demand is presented
(3) From 12.00 pm to 15.00 pm, the node is compromised and 50% increase in demand is presented

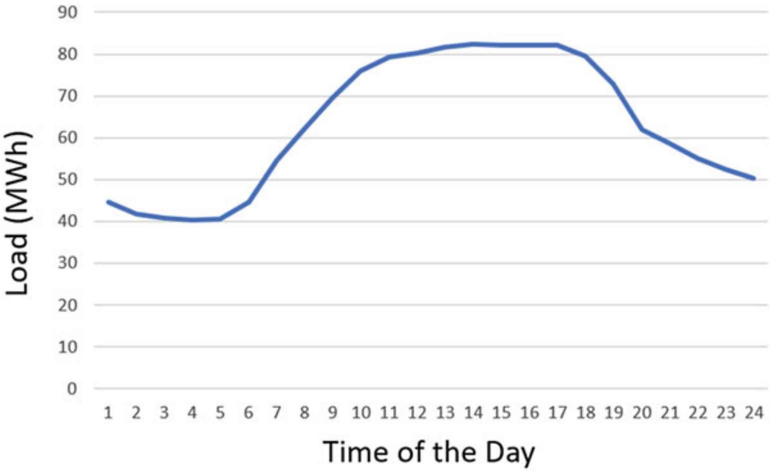

Fig. 10 Actual Demand signal for the tested day

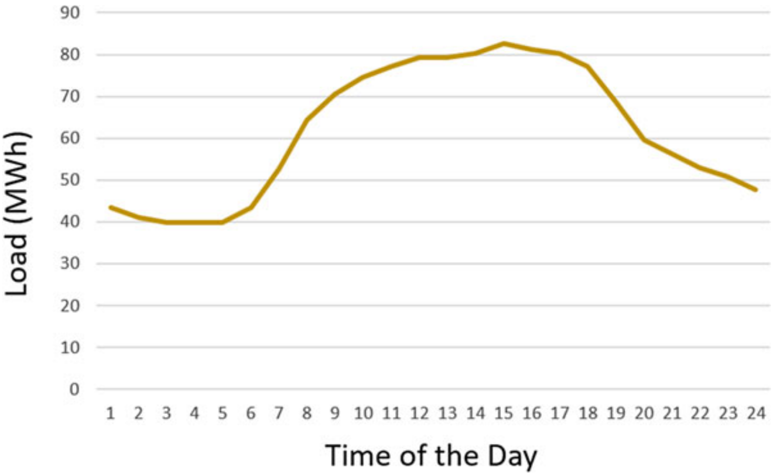

Fig. 11 Anticipated by GPR signal for the tested day

(4) From 12.00 pm to 15.00 pm, the node is compromised and 75% increase in demand is presented

(5) From 12.00 pm to 15.00 pm, the node is compromised and 90% increase in demand is presented.

The presented intelligent system is applied in the above scenarios and a degree of confidence per hour is taken. The respective degrees of confidence are given in Table 1. We observe in Table 1, that in the majority of the cases the intelligent system provides low confidence with regard to confidence of compromise. The value is not zero, mainly because of the uncertainty in load prediction and the volatility of

Table 1 Results obtained for the five tested scenarios

Time	Confidence of compromise				
	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5
12.00 am	0.20	0.20	0.20	0.20	0.20
1.00 am	0.20	0.20	0.20	0.20	0.20
2.00 am	0.20	0.20	0.20	0.20	0.20
3.00 am	0.20	0.20	0.20	0.20	0.20
4.00 am	0.20	0.20	0.20	0.20	0.20
5.00 am	0.20	0.20	0.20	0.20	0.20
6.00 am	0.20	0.20	0.20	0.20	0.20
7.00 am	0.20	0.20	0.20	0.20	0.20
8.00 am	0.20	0.20	0.20	0.20	0.20
9.00 am	0.20	0.20	0.20	0.20	0.20
10.00 am	0.20	0.20	0.20	0.20	0.20
11.00 am	0.20	0.20	0.20	0.20	0.20
12.00 pm	0.20	0.31	0.74	0.80	0.88
1.00 pm	0.20	0.35	0.74	0.82	0.90
2.00 pm	0.20	0.31	0.72	0.80	0.88
3.00 pm	0.20	0.31	0.72	0.80	0.88
4.00 pm	0.20	0.20	0.20	0.20	0.20
5.00 pm	0.20	0.20	0.20	0.20	0.20
6.00 pm	0.20	0.20	0.20	0.20	0.20
7.00 pm	0.20	0.20	0.20	0.20	0.20
8.00 pm	0.20	0.20	0.20	0.20	0.20
9.00 pm	0.20	0.20	0.20	0.20	0.20
10.00 pm	0.20	0.20	0.20	0.20	0.20
11.00 pm	0.20	0.20	0.20	0.20	0.20

prices, as well as in the defuzzificaton method. The center of area method does not get the extreme values (0 and 1). However, a low confidence is an adequate sign to make the operator believe that there is no cyberattack. Though there is no specific decision threshold, any confidence value above 0.7 denotes a certain occurrence of node compromise.

Regarding the scenarios that we have intentionally increased the demand following the goal of the attack (to make the node blackout), we observe the result in the shaded area at the center of Table 1. We observe in scenario 2 that the confidence slightly increases. This increase is very small and therefore the operator may ignore it. However, the amount of load that was compromised is only 10% and thus we assume that this is not enough to cause serious problem to that node. Overall, this compromise may not be detected; however, the goal of the system is to support stakeholders in decision-making tasks, rather than making the actual decisions.

With regard to scenarios 3,4 and 5 the confidence increases above 0.7 and therefore we can consider that a cyberattack has been detected with high confidence. Such high confidence is a serious indicator that something is wrong, and the demand increased beyond the regular one. Therefore, it safe to conclude that the intelligent system presented detects the threat in those cases with high confidence and hence, it supports the correct decision by the operator.

6 Conclusions

Smart power systems are systems that integrate power with information, and as a result may become targets for cyberattackers. The importance of the power grid for innumerable everyday activities and modern life makes the defense of the grid mandatory. In addition, recent recorded attacks showed that cyberattacks may be carefully planned and not just opportunistic cases for attackers to show off. Therefore, every aspect of smart power systems should be secured.

Intelligent systems offer new opportunities for implementing new decision support and data analysis methods that mimic the way of human system operators. In this work, we examined the case in which the attacker plans to congest a power grid node by increasing the demand and causing a blackout. An intelligent system that learns from load signals by utilizing GPR and fuzzy inference was developed and applied on a set of five different scenarios. The results were encouraging: the higher the “compromised demand” the higher the degree of confidence that the system is being compromised provided by our system. Therefore, our system shows a high potential for its deployment into smart power systems, and in particular for an Energy Internet scenario is high.

Future work will contain two main directions. In the first direction, we will explore the use of other kernel function beyond the Gaussian kernel for prediction making in the GPR model. In particular, we will apply a variety of kernels on load data from coming from different nodes, and record their performance. Analysis of records will be used to develop a system for indicating the best kernel for each node. In the second direction, we will extensively test our intelligent systems in a higher variety of data including data of nodes from different geographical areas, and different assembly of customers.

References

1. Wood, A. J., & Wollenberg, B. F. (2012). *Power generation, operation, and control*. John Wiley & Sons.
2. Amin, S. M., & Wollenberg, B. F. (2005). Toward a smart grid: power delivery for the 21st century. *IEEE power and energy magazine*, *3*(5), 34–41.
3. Han, Y., & Song, Y. H. (2003). Condition monitoring techniques for electrical equipment-a literature survey. *IEEE Transactions on Power delivery*, *18*(1), pp. 4–13.

4. Li, S., Li, C., Chen, G., Bourbakis, N. G., & Lo, K. T. (2008). A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. *Signal Processing: Image Communication*, *23*(3), pp. 212–223.
5. Ramsey, B. W., Stubbs, T. D., Mullins, B. E., Temple, M. A., & Buckner, M. A. (2015). Wireless infrastructure protection using low-cost radio frequency fingerprinting receivers. *International Journal of Critical Infrastructure Protection*, *8*, 27–39.
6. Alamaniotis, M., Gao, R., & Tsoukalas, L.H., "Towards an Energy Internet: A Game-Theoretic Approach to Price-Directed Energy Utilization," in *Proceedings of the 1st International ICST Conference on E-Energy*, Athens, Greece, October 2010, pp. 3–10.
7. Alamaniotis, M., Bargiotas, D., & Tsoukalas, L.H., "Towards Smart Energy Systems: Application of Kernel Machine Regression for Medium Term Electricity Load Forecasting," *SpringerPlus – Engineering*, Springer, vol. 5 (1), 2016, pp. 1–15.
8. Karnouskos, S. (2011, July). Cyber-physical systems in the smartgrid. In *Industrial Informatics (INDIN), 2011 9th IEEE International Conference on* (pp. 20-23). IEEE.
9. Alamaniotis, M., & Tsoukalas, L.H., "Implementing Smart Energy Systems: Integrating Load and Price Forecasting for Single Parameter based Demand Response," *IEEE PES Innovative Smart Grid Technologies, Europe (ISGT 2016),* Ljubljana, Slovenia, October 9-12, 2016, pp. 1–6.
10. Beaver, J. M., Borges-Hink, R. C., & Buckner, M. A. (2013, December). An evaluation of machine learning methods to detect malicious SCADA communications. In *Machine Learning and Applications (ICMLA), 2013 12th International Conference on* (Vol. 2, pp. 54–59). IEEE.
11. Kesler, B. (2011). The vulnerability of nuclear facilities to cyber attack. *Strategic Insights*, *10*(1), 15–25.
12. Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the cyber attack on the Ukrainian power grid. *SANS Industrial Control Systems*.
13. NUREG/CR-6882, (2006). Assessment of wireless technologies and their application at nuclear facilities. ORNL/TM-2004/317.
14. Song, J. G., Lee, J. W., Lee, C. K., Kwon, K. C., & Lee, D. Y. (2012). A cyber security risk assessment for the design of I&C systems in nuclear power plants. *Nuclear Engineering and Technology*, *44*(8), 919–928.
15. Goel, S., Hong, Y., Papakonstantinou, V., & Kloza, D. (2015). *Smart grid security*. London: Springer London.
16. Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2012). Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, *100*(1), 195–209.
17. Lu, Z., Lu, X., Wang, W., & Wang, C. (2010, October). Review and evaluation of security threats on the communication networks in the smart grid. In *Military Communications Conference, 2010-MILCOM 2010* (pp. 1830–1835). IEEE.
18. Dondossola, G., Szanto, J., Masera, M., & Nai Fovino, I. (2008). Effects of intentional threats to power substation control systems. *International Journal of Critical Infrastructures*, *4*(1-2), 129–143.
19. Taylor, C., Krings, A., & Alves-Foss, J. (2002, November). Risk analysis and probabilistic survivability assessment (RAPSA): An assessment approach for power substation hardening. In *Proc. ACM Workshop on Scientific Aspects of Cyber Terrorism,(SACT), Washington DC* (Vol. 64).
20. Ward, S., O'Brien, J., Beresh, B., Benmouyal, G., Holstein, D., Tengdin, J.T., Fodero, K., Simon, M., Carden, M., Yalla, M.V. and Tibbals, T., 2007, June. Cyber Security Issues for Protective Relays; C1 Working Group Members of Power System Relaying Committee. In *Power Engineering Society General Meeting, 2007. IEEE* (pp. 1–8). IEEE.
21. Alamaniotis, M., Chatzidakis, S., & Tsoukalas, L.H., "Monthly Load Forecasting Using Gaussian Process Regression," *9th Mediterranean Conference on Power Generation, Transmission, Distribution, and Energy Conversion: MEDPOWER 2014*, November 2014, Athens, Greece, pp. 1–7.

22. Qiu, M., Gao, W., Chen, M., Niu, J. W., & Zhang, L. (2011). Energy efficient security algorithm for power grid wide area monitoring system. *IEEE Transactions on Smart Grid*, *2*(4), 715–723.
23. Bishop, C.M. *Pattern Recognition and Machine Learning,* New York: Springer, 2006.
24. Alamaniotis, M., Ikonomopoulos, A., & Tsoukalas, L.H., "Probabilistic Kernel Approach to Online Monitoring of Nuclear Power Plants," *Nuclear Technology*, American Nuclear Society, vol. 177 (1), January 2012, pp. 132–144.
25. C.E. Rasmussen, and C.K.I. Williams, *Gaussian Processes for Machine Learning,* Cambridge, MA: MIT Press, 2006
26. D.J.C. Mackay, Introduction to Gaussian Processes, in C. M. Bishop, editor, *Neural Networks and Machine Learning*, Berlin: Springer-Verlag, 1998, vol. 168, pp. 133–155.
27. Tsoukalas, L.H., and R.E. Uhrig, *Fuzzy and Neural Approaches in Engineering*, Wiley and Sons, New York, 1997.
28. Alamaniotis, M, & Agarwal, V., "Fuzzy Integration of Support Vector Regressor Models for Anticipatory Control of Complex Energy Systems," *International Journal of Monitoring and Surveillance Technologies Research,* IGI Global Publications, vol. 2(2), April-June 2014, pp. 26–40.
29. Consortium for Intelligent Management of Electric Power Grid (CIMEG), http://www.cimeg.com
30. Alamaniotis, M., & Tsoukalas, L., "Layered based Approach to Virtual Storage for Smart Power Systems," in *Proceedings of the 4thInternational Conference on Information, Intelligence, Systems and Applications,* Piraeus, Greece, July 2013, pp. 22–27.
31. Alamaniotis, M., Tsoukalas, L. H., & Bourbakis, N. (2014, July). Virtual cost approach: electricity consumption scheduling for smart grids/cities in price-directed electricity markets. In *Information, Intelligence, Systems and Applications, IISA 2014, The 5th International Conference on* (pp. 38–43). IEEE.
32. Tsoukalas, L. H., & Gao, R. (2008, April). From smart grids to an energy internet: Assumptions, architectures and requirements. In *Electric Utility Deregulation and Restructuring and Power Technologies, 2008. DRPT 2008. Third International Conference on* (pp. 94–98). IEEE.
33. Tsoukalas, L. H., & Gao, R. (2008, August). Inventing energy internet The role of anticipation in human-centered energy distribution and utilization. In *SICE Annual Conference, 2008* (pp. 399–403). IEEE.
34. Alamaniotis, M., & Tsoukalas, L. H. (2016, June). Multi-kernel anticipatory approach to intelligent control with application to load management of electrical appliances. In *Control and Automation (MED), 2016 24th Mediterranean Conference on* (pp. 1290–1295). IEEE.

Miltiadis "Miltos" Alamaniotis is a research assistant professor in the School of Nuclear Engineering at Purdue University since September 2014. He received his Dipl-Ing. in Electrical and Computer Engineering from University of Thessaly, Greece in 2005 and his M.S. and Ph.D. degrees in Nuclear Engineering from Purdue University in 2010 and 2012 respectively. His interdisciplinary research focuses on development of intelligent systems and machine learning approaches for smart power systems, smart cities and grids, security, radiation detection, and nuclear power plant controls. He had held a guest appointment with Argonne National Laboratory from 2010 to 2012, and was a visiting scientist in the Power and Energy Division of Oak Ridge National Laboratory in May 2016. In Fall 2015, he was honored with the "Paul C. Zmola Scholar" Award by Purdue University for his research contributions. He is an active member of the American Nuclear Society, IEEE, and has served as chair in artificial intelligence conferences.

Lefteri H. Tsoukalas is professor and former head of the School of Nuclear Engineering at Purdue University and has held faculty appointments at the University of Tennessee, Aristotle University, Hellenic University and the University of Thessaly. He has three decades of experience in smart instrumentation and control techniques with over 200 peer-reviewed research publications including the textbook "*Fuzzy and Neural Approaches in Engineering*" (Wiley, 1997). He directs the Applied Intelligent Systems Laboratory, which pioneered research in the intelligent management of the electric power grid through price-directed, demand-side management approaches, and anticipatory algorithms not constrained by a fixed future horizon but where the output of predictive models is used over a range of possible futures for model selection and modification through machine learning. Dr. Tsoukalas is a Fellow of the American Nuclear Society. In 2009 he was recognized by the Humboldt Prize, Germany's highest honor for international scientists.