Cyber Attack of a Power Grid Analysis Using a Deep Neural Networks Approach

Delia Ioana Dogaru, Ioan Dumitrache

Faculty of Automatic Control and Computer Science, University Politehnica Bucharest, Romania
di.dogaru@gmail.com, ioan.dumitrache@acse.pub.ro

Abstract: The integration of new technologies into the power grid leads to a growing, complex, interconnected system that is exposed to various cyber vulnerabilities. A power grid operating state can be altered due to the dynamic cyber-attacks which target different system objectives. This article brings forward the approach of power grid behavior analysis to identify two operating states: normal versus attacked. Once established the features for such states, we focus on Deep Neural Networks as security methods to mitigate the impact of cyber-attacks on the power grid by providing a case study simulation in MATLAB to sustain the proposed method.

Keywords: power grid; cyber-physical systems; deep neural networks; power grid; cyber-attacks; security; impact analysis.

1. INTRODUCTION

In the power grids new technologies have been developed and together with the economic trends they gave rise to the need of quality energy production and efficient delivery and consumption. One of the most developed and advanced sector is the information and communication technology (ICT), contributing greatly to the transition of the power grid into the Smart Grid (Dumitrache, 2014; Dumitrache, 2009). This transition enables a series of improvements like a better visibility of the power grid's status by introducing advanced communication and measurement techniques which allows predictive analytics for reducing peak demand and redirecting energy in an optimal way if problems occur in the network nodes, etc..

Within the power grid, the integration of ICT, advanced processing and control systems with the physical components results in an exponential increase in complexity leading to the paradigm of Cyber – Physical Energy System (CPES) (Dumitrache, 2013), attracting numerous cyber vulnerabilities that can be exploited.

Although, the ICT domain already has structured cyber security policies addressing existing vulnerabilities, analysed and evaluated in their own data systems, the same vulnerabilities need to be evaluated by the degree and type of impact they have on the power grid because the direct impact is on the physical components. Moreover, as the complexity of the smart grid increases, so does the rise of new ways of cyber hacking launching more adaptive and dynamic methods that can compromise normal execution of the entire power grid and for which there are no security strategies. The next generation of cyber security strategies for the ever-changing cyber threats must maintain a balance between the power grids and cyber systems and specific approaches must be considered because inappropriate implementations of cyber security applications could lead to performance degradation of the power grid. Moreover, the security methods for preventing and detecting cyber anomalies should consider the overall impact on the grid rather than just focusing on the isolated effects that cyber-attacks can have. Having both a macro and micro analysis and monitoring of what is happening in the power grid at any given time increases the chances for anomaly detection and prevention by covering a wider range of scenarios.

Cyber-attacks can target any power grid level from generation, transmission and distribution, to consumers, and based on the impact of the attack, the effects can be locally or cascading through the system. In our previous article (Dogaru, 2017) different types of attacks on the power grid are presented and their impact on the generation, transmission, distribution and consumption. Also, some stability concerns (rotor speed, voltage, frequency stability) are analysed when the power grid faces different classes of cyber-attacks to underline their severity on different levels: control, communication, software, hardware. But, cyber-attacks are continuously adapting in response to the new developments of the power grids.

Most methods for preventing or detecting these intrusions rely on an outdated arsenal of techniques that are inherited from the IT domain and adopted in an insufficient manner to the needs of the complex real-time CPS in the power domain. These normal techniques focus on existing types of attacks - e.g. Load Redistribution[1] (Dogaru, 2017), Distributed Denial of Service[2] (Dumitrache, 2015), etc., their entry points (ports,

[1] Load Redistribution (LR) attack is a type of False Data Injection attack targeting to inject load bus and line power data.

[2] Denial-of-service (DoS) attacks target TCP/IP based protocols (e.g., IEC 61850) altering (damage, block or delay) the communication in the Smart Grid.

wireless communication, etc. - and target (command signals, sensor data, log data, etc.).

The assessment of a real-time system from a security point of view to determine the cyber vulnerabilities proves to be challenging due to the fact that the current conventional technology is computationally expensive and slow for a dynamic system such as the power grid. We consider the machine learning techniques, having pattern recognition capabilities and high-speed learning, to be most suitable for security assessment of a power grid.

In the complex and dynamic computer environments machine learning, specifically techniques like Artificial Neural Networks (ANN) are ideal for prediction and classification for different tasks including security assessments as mentioned in some studies like analysing denial of service (DoS) attacks by applying neural networks in the work of Itikhar, (Itikhar, 2009). Their results are better than any other studies having a good rate of detection. A very robust spam filtering method was introduced in the work of Wu (Wu, 2009) using a hybrid method of rule-based processing and back-propagation neural networks. In the articles (Bitter, 2010; Itikhar, 2009; Wu, 2009), an intrusion detection system is presented host-based and network-based with special focus on artificial neural networks to identify suspicious and potentially malicious traffic.

Deep structured learning, part of the more advanced machine learning methods, with focus on deep artificial neural networks for cyber security assessment of a power grid is a new approach that few studies conducted. In the article (Semitekos, 2002) a toolkit was developed containing machine learning and analysis tools to perform a security assessment on a power grid. This toolkit is developed for steady state contingency analysis and covers branch and bus outages only. The results achieved are encouraging, and as stated in the article there are a number of possible improvements that can still be made.

Another example of machine learning used in security assessment of power grids is the article (Tomin, 2016) where different deep learning techniques (e.g. ANN, decision trees, etc.) are tested on-line in order to find the best algorithm based on its top performance for a particular power grid, like the IEEE RTC-96.

Malicious code like trojans, worms, malware, etc. , is a code attached in a software system with the potential to create an undesired effect. Due to its impact that it has in damaging the system and level of sophistication, it cannot be efficiently detected and contained just by an antivirus program. Several researches (Zhang, 2011; Chaudhari, 2017) have used feature extraction for malicious code behaviour, but due to the algorithms high complexity and low rate of detection, they prove to be not suitable for real world implementation. Another study (Li, 2015) has increased the detection rate scoring a high accuracy by introducing Deep learning into the equation, proposing a hybrid model for malicious code detection.

Although these studies present good results, we consider a different approach based on the motivation that attacks should be regarded not only from their local impact or sole target in the power grid, but rather from the perspective where a combination of attack types in a distributed manner can inject or alter system information, which combined, can cause an overall abnormal system behaviour. Taken separately, they have no impact neither locally nor globally, but together they can create an overall cascading effect.

In this paper, the focus is on analysing the overall modelled behaviour of a power grid using the deep learning technique, deep neural networks, to identify abnormal behaviour due to cyber-attacks targeting different levels of the grid. In Section II we define machine learning methods, deep learning and motivate our choice for its usefulness in identifying malicious behaviour of a power grid. In Section III the multi-machine model dynamics, IEEE-9 bus, chosen for the case study is described. Section IV presents the DNN methodology for implementing security assessment of the power grid's behaviour along with the simulation of the proposed model carried out in MATLAB to predictively identify abnormal/malicious behaviours when the grid is subjected to cyber-attacks.

2. DEEP STRUCTURED LEARNING AND WHY DEEP NEURAL NETWORKS

Due to the high integration of communication and information technologies in the power grid, an extra layer has emerged at every level of the grid – generation, transmission, distribution, consumption – enabling the acquisition, storage, analysis of data though networked sensors, measuring and processing units to improve quality production and delivery of power. This layer determines high volumes of data which utility companies need to manage with appropriate tools. The term that best describes the set of high volumes of data managed only by advanced methods of analysis and knowledge extraction on high power processing units is "Big Data".

The accelerated increase in data volumes due to the evolution of complex interconnection of cybernetic and physical components imposes major challenges in designing and managing the complex, physical-cybernetic systems within the energy networks in several aspects, such as performance, energy efficiency, security, reliability, durability, tolerance, scalability and flexibility.

The availability of large data volumes due to the proliferation of intelligent smart grids in smart grids paves the way for implementing the large data concept in detecting and preventing security incidents by analysing multiple network entries that look for patterns or anomalies by extracting features (distinctive properties from an initial set of input data).

The large input of data consists in the possibility of extracting information from large data collected from different sources - data packets, servers, logs, sensor data, etc. - using a

correlation analysis to give meaning to the links between the multitude of data. Extracted information from advanced processing can be used to determine power grid behaviours, that can be classified into normal and abnormal behaviours. The potential in analysing cases of normal behaviour and abnormal behaviour based on historical and real-time data will lead to building of knowledge databases, transforming security strategies into evolved strategies with intelligent decision-making capabilities in detecting abnormal power grid behaviours under the influence of cyber-attacks.

In security assessment and risk mitigation Big data is beginning to be applied due to the high integration of intelligent measuring devices for detecting system anomalies, operating patterns, etc. Using Big Data in cyber security we believe data should be passed through the following steps:

- **Data classification** based on a sensitivity level. Data comes from all kinds of sources and contain various information. This needs to be classified based on their importance and high risk if they were ever in the case to be captured by an unauthorized party;
- **System classification** based on a sensitivity level. The power system must be divided in sections and classified according to their vulnerability level. Vulnerability must be regarded in terms of entry points, cybernetic risk and impact in case of security breach;
- **Encryption** – transfer packets of data need to be encrypted to eliminate any vulnerability regarding packet interception or eavesdropping and even false data injection;
- **User access** should be closely monitored. Also, users, based on their role should be granted access on certain levels sensitive data;
- **Strategic plans** need to be thought in any scenario case in which data can be manipulated and the effects of this action has on the overall system;
- The whole system should be **continuously monitored** because attacks on data can have a varied overall impact.

We believe that big data can be used to analyse in depth the response behaviour of a power grid or a communication network by identifying the normal state of operations and the abnormal state by introducing cyber disturbance, such as cyber-attacks. This would provide a valuable information of the overall state of the system in terms of security. Although a lot of the cyber-attacks that target the power grid are inherited from the IT domain, the existing methods for mitigating their risks are insufficient because the attacks evolve becoming more complex, adaptive and dynamic. Various forms can alter system data in a distributed manner and can have a targeted impact.

Machine learning is the application of artificial intelligence through a set of methods based on the idea that machines can learn from data to identify models and learn without a priori programming to execute specific tasks and make decisions. This is part of artificial intelligence domain, that began from pattern identification. Machine learning techniques are not new, but the ability to apply complex mathematical calculations on high volumes of data in a fast timely and computational manner is something recent.

Deep learning or Deep Neural Networks (DNN) is a machine learning technique, one of the most active research areas due to its impressive mathematical foundation used in many domains to solve complex problems and, also, in power grids for fault diagnosis (e.g. recognizing transient events in nuclear power plants to anticipate accidents) (Lukic, 2013), forecast of peak electric loads (Germond, 2013; Khadem, 2013), identification, modelling and prediction (Samad, 2013), control of load shedding and real-time stability analysis (Novosel, 2013), etc..

Deep structured learning is comprised of a series of learning algorithms intended to mimic the biological brain into engineered systems models to allow computers to understand the world in terms of a hierarchy of concepts and to learn from experience the relation between each concept.

Due to their adaptability in dealing with various types of data, their parallel processing capability allows increased speed in computation and high accuracy in making predictions, deep neural networks (DNN) are successful in modelling many non-linear systems and are suitable for real-time applications. Their applicability expands to pattern recognition, classification, anomaly recognition, clustering imprecise data.

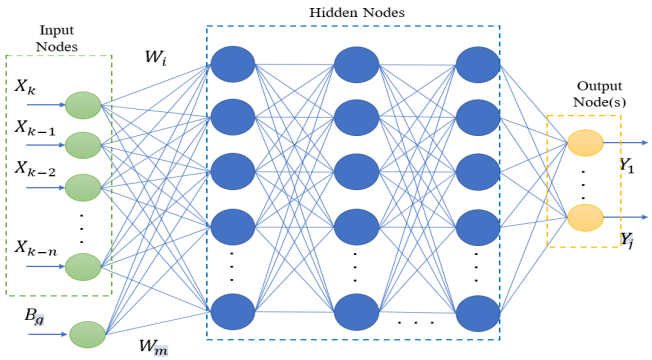

Fig. 1. Deep neural network structure.

Deep Neural Networks is a machine learning-based technique derived from the well-known Neural Networks and related algorithms (for supervised, unsupervised and semi-supervised learning) which process through many layers of nonlinear transformations very raw input data to obtain the desired output.

The overall increase in its emergent behaviour is due to the highly interconnected processing elements – neurons or nodes, organized in layers (input layer, hidden layers and output layer), each containing weights and biases and an activation function for the training process and data convergence, as in figure 1. Learning means adjusting the weights to reduce the error between the target output and actual outputs. The activation function can be linear or non-linear. If we try to fit non-linear data choosing a linear activation function for the layers than the best approximation of the data will be linear and will result in low performance. If the network is complex enough it can learn any function.

The cyber infrastructure in the power grids is highly vulnerable to cyber threats due to increased complexity and integration of heterogenous components. Traditional methods for security assessment and human intervention are not sufficient for its protection.

Cyber-attacks are continuously evolving and adapting to the new implementations in the power sector. They can be centralized, compromising, locally, a single device and with cascading effect because the system is interconnected, or distributed, targeting multiple devices which can be geographically dispersed and having also a possible cascading effect. Thus, comes the need for a strategy more adaptive to any problem, flexible, robust, capable of handling and learning from high volume and high-dimensional data sets coming from various sensors and measurement devices and able to provide accurate solutions to threats in real-time.

The power grid is a large-scale system expressed in the form of nonlinear differential equations which consume a lot of computational processing power. To handle such a complex system defined by complex mathematics, we consider "deep neural networks" – DNN – as the best approach to model the relationship between input data and output data where knowledge of prior features is less known. DNN use less computational power and are more time efficient without the need of a complete set of differential equations, using pre-calculated results for training and obtaining accurate solutions (Swain, 2006).

3. DYNAMICS OF THE POWER GRID

The electric grid is a large-scale system described by various interacting control loops between physical and cyber components of nonlinear nature due to its dynamic behaviour operating on multiple time scales. Because of its complexity the analysis and control of such a system is constrained to rely on reduced models that preserve only its important aspects through Differential-Algebraic Equations (DAEs) describing generator and control systems, loads, network behaviour, other devices. A power grid is hard to accurately model because of the different time constants of the dynamic elements in the grid. One model that best describes such system and is accepted in the domain literature (Anderson, 1977) for power grid analysis control is the multi-machine model because each generator has a pre-defined model reduced to the non-linear second order differential equation for describing the swing of the generator's rotor in interaction with the grid (Arghir, 2016).

We consider the IEEE 9-bus system having 3 generators (one classical model and the other 2 are a two-axis model) and three active loads which is analysed in the form of linearized equations from (Anderson, 1977) in our article (Dogaru, 2018) where we present the continuous-time state-space model of the system in the nine-linear first order differential algebraic equations form, equation (4).

The power grid model (chosen IEEE 9 bus) is a non-linear system that can be approximated by a linear one to better study its properties near a region of operation. The state dynamics of the power grid is described as a linear time invariant system of $u \epsilon R^n$ input control signals and $y \epsilon R^m$ output signals captured as measurements in continuous time by sensors (or PMUs) and subjected to cyber-attacks, disturbances and faults. The DAE equations are:

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) + P(t)d(t) + c \\ y_q(t) = C_q x(t) + v_q(t) \\ d(t) = [u_d(t)\ f_f(t)] \end{cases} \quad (1)$$

Where: $A \in R^{3n_g x 3n_g}$, $B \in R^{3n_g x\, m_1}$, $C_q \in R^{qx3n_g}$, $P \in R^{3n_g x m_2}$ (the disturbances and faults against the actuator matrix), $u_d(t)$ is the input disturbance, $f_f(t)$ is the actuators fault and both are considered unknown inputs. C denotes the output matrix, q is the number of buses where PMUs are installed, 3^{n_g} represents the states of the generators (rotor angles, rotor speeds, voltages), m_1 known grid inputs (mechanical input power and field voltage), m_2 unknown grid inputs and q output measurements. $v_q(t)$ is the potential vector against the output of the system measured by the PMUs or sensors and sent to the control centres (Dogaru, 2018).

The state vector which must represent the whole range of system operating states is:

$$x^T - [\omega_1 \quad E'_{q2} \quad E'_{d2}\ \omega_2 \quad E'_{q3} \quad E'_{d3}\ \omega_3 \quad \delta_{12} \quad \delta_{13}] \quad (2)$$

And the input of the system:

$$u^T = [T_{m1} \quad E_{FD2} \quad T_{m2} \quad E_{FD3} \quad T_{m3}] \quad (3)$$

Thus, using the details in (2018, Dogaru) along with the equations 1-3, the continuous-time state-space model of the system is in the following form being comprised of nine-linear first order differential algebraic equations (4):

$$[\dot{\omega}_1 \quad \dot{E}'_{q2} \quad \dot{E}'_{d2}\ \dot{\omega}_2 \quad \dot{E}'_{q3} \quad \dot{E}'_{d3}\ \dot{\omega}_3 \quad \dot{\delta}_{12} \quad \dot{\delta}_{13}]^T$$

$$= 10^{-4} \begin{bmatrix} -0.561D_1 & 0.6793 & 0.6099 & 0 & 0.4948 & 0.5463 & 0 & -0.952 & -0.7494 \\ 0 & -13.7658 & 1.4409 & 0 & 3.6163 & 1.1781 & 0 & 8.5472 & -3.3161 \\ 0 & -15.5076 & -150.1554 & 0 & -12.6793 & 38.9205 & 0 & 42.4023 & -21.4333 \\ 0 & -6.5352 & -1.1714 & -2.0723D_2 & 0.9552 & 2.2156 & 0 & 5.4592 & -2.3385 \\ 0 & 5.6334 & 0.4076 & 0 & -16.5675 & 1.4111 & 0 & -4.2309 & 10.1170 \\ 0 & -3.8073 & 52.627 & 0 & -13.1829 & -156.9117 & 0 & -38.8349 & 68.5987 \\ 0 & 2.9781 & 3.9766 & 0 & -10.6238 & -4.7247 & -4.4063D_3 & -5.2010 & 10.7116 \\ 10000 & 0 & 0 & -10000 & 0 & 0 & 0 & 0 & 0 \\ 10000 & 0 & 0 & 0 & 0 & 0 & -10000 & 0 & 0 \end{bmatrix} \begin{bmatrix} \omega_1 \\ E'_{q2} \\ E'_{d2} \\ \omega_2 \\ E'_{q3} \\ E'_{d3} \\ \omega_3 \\ \delta_{12} \\ \delta_{13} \end{bmatrix}$$

$$+ [0.561T_{m1} \quad 4.421E_{FD2} \quad 0 \quad 2.0723T_{m2} \quad 4.5035E_{FD3} \quad 0 \quad 4.4063T_{m3} \quad 0 \quad 0]^T \quad (4)$$

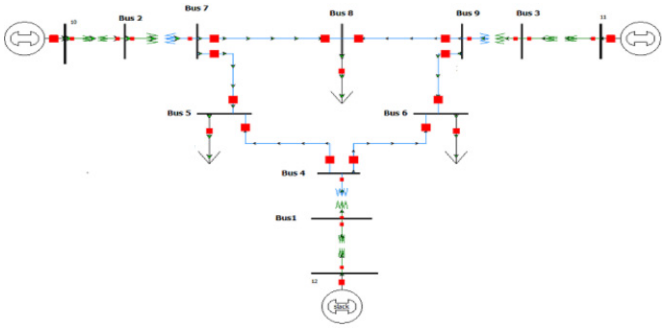

Fig. 2. IEEE 9-bus.

The IEEE-9 bus power grids benchmark model, figure 1, is used to test the proposed deep neural network approach for cyber security assessment in the following section.

4. CASE STUDY

The traditional security strategies rely upon the load flow analysis and transient stability - in terms of frequency, rotor angle, voltage stability - to identify possibly abnormal behaviours. But, these strategies are not a good solution for real time applications, considering they would be time consuming due to the high volumes of data to be computed and not convenient for a non-linear system, such as the large-scale power grid system (Kalyani, 2009).

In this study, we focus on capturing the underlying behavioural features of the power grid and use them to detect any cyber-attack by simulation in MATLAB/Simulink using deep neural networks. We choose the dynamic nonlinear autoregressive neural network (NAR), closed loop feedback, because it accepts dynamic inputs without the need of having knowledge about the process, making it a suitable solution in using it for the power grid described by a non-linear function due to its complexity and interdependencies.

The chosen NAR is a 12-layer network, having the Levenberg-Marquardt training function. This network was trained in MATLAB for 300 epochs having a training goal of having the error less than 0.001.

Another reason for choosing deep neural networks is the resilience to noisy data, and the ability to classify patterns on first hand data sets without a prior training (Kalyani, 2009).

The power grid is described from the proposed multi-machine model in Section 2, IEEE-9 bus, figure 2. The simulation and development of the DNN was made in MATLAB/Simulink environment.

Upon off-line simulation of the power grid model generated through developed programs in MATLAB/Simulink, the obtained result can be best described as a time series model, see figure 3.

This is used as data samples needed for training and testing to identify certain patterns and given the input feature vector described by the past behaviour of the power grid – time series model – to accurately predict future system behaviour.

Upon the benchmark model chosen, IEEE-9 bus, we consider a normal behaviour and a disturbed behaviour. We consider the disturbances only in the form of cyber-attacks, $v_q(t)$ as expressed in equation (1) and can occur in any form and at any level in the power grid. These can occur as bad command signals between controllers (or the control centre) and actuators or they can, also, target the output signals captured by sensors delivered to the control centres influencing the decision-making process. Disturbances can be, also, in the form of system faults and considered indistinguishable from cyber attacks because both have similar direct effects on the physical system (Barabanov, 2016). We focus on cyber attacks because they can dynamically adapt to the target system and are continuously evolving. Being able to identify or anticipate a system suffering from the effects of such attacks can have a major impact in developing appropriate security measures to overcome critical situations. Cyber attacks have a wide range of classes that target:

- To change the output measurements captured by sensors or PMUs so that false ones can be sent to the control center (which monitors and controls the grid) or to alter the control commands and manipulate the course of action with varying levels of risk;
- To modulate power consumption of connected devices to the grid in a coordinated way to determine unpredictable fluctuations at very large scales causing unscheduled load-shedding (Dabrowski, 2017);
- To interrupt or delay the communication from the sensors to the control center or the signal command from the control center to the actuators;
- To gain access to architectural information of the power grid to have real-time operation visibility and possibly destroy stored data on servers, etc. .

The normal behaviour of the power grid is simulated and shown in a timeframe of 1000 seconds:

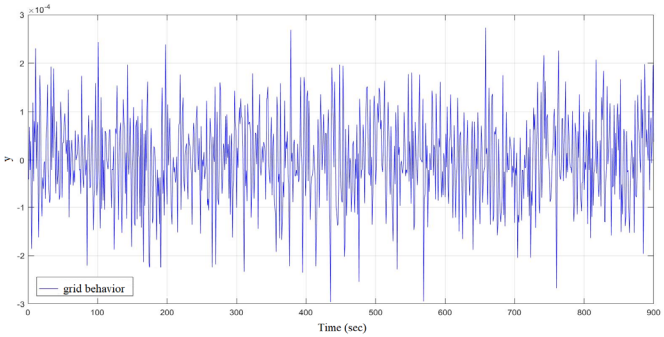

Fig. 3. Normal behaviour of the power grid.

Stages of the simulation:

- The state-space mathematical representation of a power grid model to identify its behaviour and obtain the input training and testing set. This was done in a previous article (Dogaru, 2018);

The DNN construction for the prediction of the grid's behaviour begins by choosing the split point for training data – interval [0;600) – and testing data set – interval [600;1000]

- Data extraction for learning/training and testing

The input data represents 2 operating states of the power grid:

  - Normal behaviour input data on which the neural networked is trained to recognize;
  - Attacked behaviour input data which the neural network should identify after its training;

- The training phase is performed off-line as it is time-consuming, for 300 epochs having a training goal of an error less than 0.001;

- The detection phase – for a given behaviour (attacked or normal), the DNN structure identifies the classification with the trained parameters.

So, upon the time horizon after the simulation we have split it to have the normal behaviour represented in blue and the predicted horizon from T = 600 sec using DNN simulated and shown in the below image in green colour.

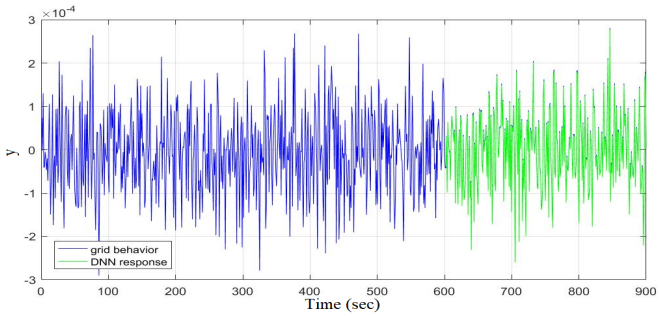

Fig. 4. Normal behaviour simulated along with the predicted behaviour of the power grid.

Attacks come in many forms and with different effects locally or globally. For instance, the local measurements from field devices (Intelligent Electronic Devices, Remote Terminal Units, Power Line Carriers and Master Terminal Units) can be altered leading to wrong estimates of state variables. Because important systems that handle the stability of the operating conditions depend on such estimates (like Optimal Power Flow (OPF), Automatic Generator Control (AGC), etc.) the consequences can result in cascading failures and performance issues and sometimes in system overloading resulting in blackouts (Dogaru, 2018).

Once the neural network is trained so that it can predict with a certain degree of accuracy the future behaviour of the power grid using the chosen mode, we can feed the attacked data so as to test it in identifying the abnormal behaviour.

The simulated behaviour of the chosen model when faced with cyber-attacks is shown in the following figure represented in magenta along with the predicted output given by the DNN in green and having the normal behaviour in blue:

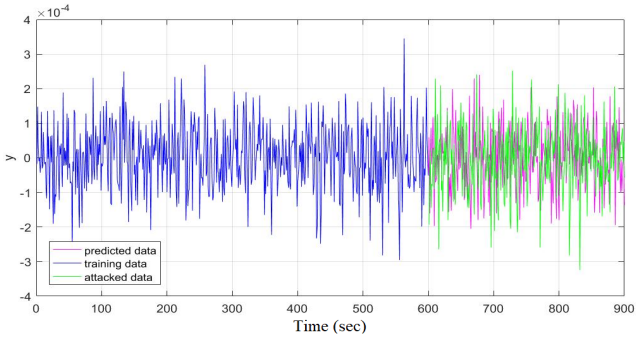

Fig. 5. Normal behaviour attacked behaviour and predicted behaviour of the power grid.

In this case, we can calculate the delta values of these two states and can observe that an abnormal behaviour is occurring and that the power grid is subjected to disturbances possibly of cyber nature.

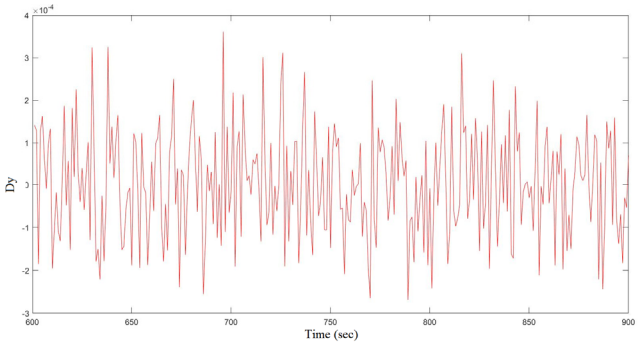

Fig. 6. Delta value between the predicted behaviour and the attacked behaviour of the power grid.

In other cases, attacks can create the illusion that the grid's behavior is normal as you can see in the figure below, figure 7, where the predicted response and the attacked response have slight differences that may not trigger any alarm and can have a local impact rather than a global disruptive effect. Some attack vectors may be specifically design so as to not trigger any alarm but, rather, have a silent and impactful effect upon the grid.

Having this stated it is necessary to establish a threshold of whether the power grid is in danger of having equipment failure or any other failure that can lead to blackouts. This can be done by an extensive training with historical data representing normal operational state and the disrupted state of the power grid. This is an ongoing process that increases in accuracy with extensive training based on huge volumes of datasets depicting various cases (normal behavior and attacked behavior by different types of attacks having different types of outcomes on the power grid).

Once the deep neural network is properly trained it can be used in the on-line evaluation, being fed real time system data to establish whether the system state is either normal or attacked. In case of the latter, a system alarm can be triggered to alert that the threshold has been reached and let the control centre know in order to take appropriate actions.

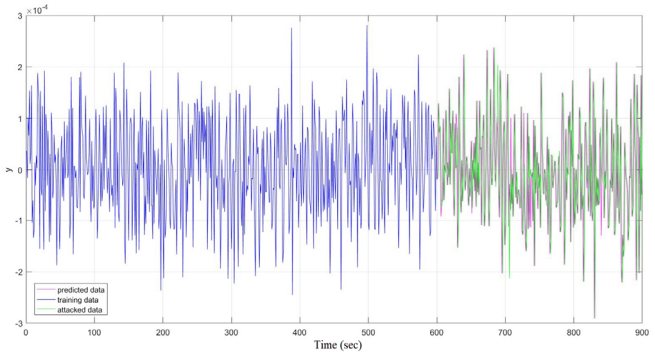

Fig. 7. Normal behavior, attacked behavior and predicted behavior of the power grid.

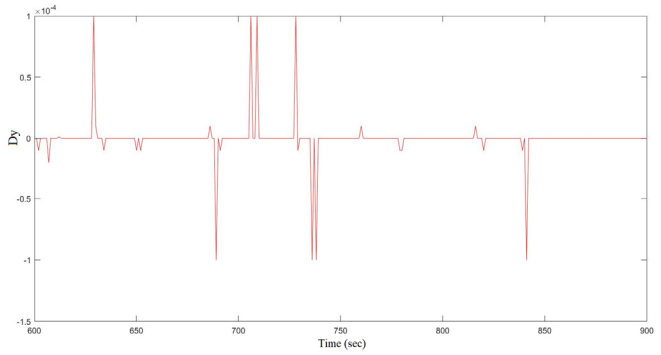

Fig. 8. Delta value between the predicted behavior and the attacked behaviour of the power grid.

5. FURTHER DISCUSSIONS

In reference (Dogaru, 2017) we analyse stability concerns – voltage, rotor angle and frequency stability - when the power grid faces different classes of cyber-attacks through simulations in MATLAB/Simulink for underlining the impact that cyber-attacks have on each level: generation, transmission, distribution and consumption. Thus, each communication channel used in the grid may present vulnerabilities exploited by cyber-attacks which can target any level of the energy system:

- Generation - attacks at this level aim to control the generators;
- Transmission - attacks are performed indirectly by false data injection to the status estimator. But the only constraint for these attacks to be successful is to abide by Kirchoff's laws. This can be achieved by accessing information about the operating parameters of the entire energy system;
- Distribution - in the energy system, the availability of real-time data is essential for accurate monitoring and for the operator to be able to act accurately according to the current state. A cyber-attack seeks to change the phase or other information about the status of the system or the redirection of the load into the network;
- Consumption - the exponential increase in load on critical nodes in the power grid leads to overloading of the system, interruptions or equipment failures

The communication channels are varied, having standards and protocols most of which are adopted from the IT domain (TCP/IP, Ethernet, UDP, etc.). This results in inheriting the same vulnerabilities, but due to the proactivity in the IT domain, there are a lot of security measures to cover almost every aspect of any cyber-attack. However, in the power grid, communication of data used in the control network has other specific industrial protocols designed just for a fast data exchange. In the context of the control network data transfer refers to the two types of critical data being exchanged:

- data signals from sensors to the control system
- data signals containing commands from the control system to the actuators.

Most used standards and protocols used in the control network are RS232, Ethernet, DNP3.0, IEC 61850, ICCP, UCA2.0 and Modbus. These are used, for example, between remote terminal units and intelligent electronic devices or in the communication between the control center and the governor control and automatic voltage regulator to transfer the reference points. Also, most of them are used in SCADA/EMS.

Although, they were design for efficiency and reliability, because of the growing power grid complexity, the need for encryption and authentication became a stringent necessity. The lack of security features leads to the rise of vulnerabilities and discovery of exploits.

Lack on encryption can lead to an easy interception and manipulation of data through packet sniffing, eavesdropping and/or side channel attacks, false data injection, etc.

Lack of authentication can lead to exposure of sensitive data regarding control signals or topology information.

There are about 200 such protocols that allow real time transfer, but the most common are (Zhu, 2011):

• Modbus - a standard protocol in industrial networks. as stated above, it does not have any security mechanism or message encryption method, which allows a cyber-attack to exploit its vulnerabilities: using the denial-of-service to reboot a Modbus server and change its configuration or shutdown, and by using the reconnaissance attack for unauthorized access of transmitted data;

• DNP3 (Distributed Network Protocol, version 3.0) used primarily in power grids as communication protocol between control centers and SCADA, RTU, MTU, PLC. The protocol is based on a simplified model of ISO / OSI model encompassing the data level, application level and pseudo-transport level. Although it provides a secure authentication mechanism (DNP3-SA), unlike Modbus, it still has some vulnerabilities that can be easily exploited by some cyber-attacks because of its interfacing with the TCP / IP protocol. This interface requires DNP3 to use Transport Layer Security (TLS) or Internet Protocol Security (IPsec) security along with commercial firewalls. This merger offers the advantage of confidentiality and authentication, but also because these encryption protocols, TLS and IPsec, are designed for commercial use and not for DNP3 specifications, their efficiency decreases. For example, they cannot confirm whether a command signal is valid or illegitimate (2007, Mander).

In order to adopt a strategy to ensure the security of the smart grid and to mitigate or eliminate risks and vulnerabilities, we must first understand the impact of cyber-attacks on the network in terms of stability and physical impact: analysis done in reference (Dogaru, 2017).

Moreover, security in electrical networks must strike a balance between physical systems, cyber systems, information processes, along with system functionalities and control. Besides the fact that electricity must be available at any time in the network, it must maintain a constant voltage, as some industrial processes are very sensitive to voltage variations and can lead to productivity losses (Dogaru, 2017).

We consider the best strategy for cyber security in power grid to be one that enables all available security measurements to be implemented at all levels: from upgrading communication protocols and standards to enable at least authentication and encryption of data, to installing or upgrading, where possible, system operation with security applications and finding ways of securing if not possible a device and its communication channels but rather a cluster of devices communicating with each other.

Moreover, beside these implementations, we regard deep neural networks and machine learning to be the next step for cyber security.

In reference (Kalyani, 2009) there are several Neural Networks models tested for classifying the system state as secure or insecure. Although, they provide good results, their approach is solely from the static or transient security point of view. It is, indeed, essential to evaluate the security of the power grid based on this perspective by taking into consideration the possible outcomes of perturbations upon the stability of the power grid, as we also stated above.

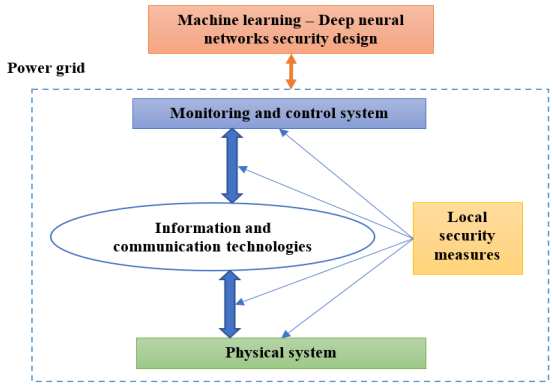

Fig. 9. Vision - Deep neural network as a future security strategy.

In our study, using the MATLAB/Simulink environment we presented the deep neural network as a security assessment solution for the complex power grid. Our vision, depicted in figure 9, is that, in conjunction to all the local security measures that could be implemented, an additional security level as an overseer of the whole power grid must be adopted through the use of deep neural networks. These are capable of running in real time and though intensive training with historical and current data it can become a copy of the power grid model in a normal operating state. In case of cyber disturbance (or any other type) individually or grouped and distributed, it can identify the abnormal behaviour by comparison. Once identified, it can trigger, as a alerts to the control centre, or through additional implementations it can take corrective actions.

6. CONCLUSIONS

The power grid is a real-time complex critical infrastructure with many interdependencies and vulnerabilities continuously developed and exposed to disturbances (small or large) that can lead, based on their nature (e.g. system disturbances, cyber disturbance, intensity and target) to system instability and ultimately to blackouts. There are security strategies to monitor the physical behaviour of the grid's components to determine whether they are being manipulated abnormally by cyber-attacks, but as seen in the literature it is hard to establish the validity of signals and commands if they come from a viable source.

The NAR model is designed, trained and used for testing with the help of the MATALB neural network toolbox and functions. The training is done with the Levenberg-Marquardt function and from various trials the most promising results were obtained by using 12 hidden layers.

We strongly underline the importance of approaching the power grid's cyber security from an intelligent approach using machine learning techniques due to their flexibility and high computational parallelism suitable for the real-time power grid. Through this approach we focused on having deep neural networks based on pattern matching to classify the secure and insecure status of the power grid for specific contingencies based on the pre-contingency system status.

The success of pattern recognition of system behaviour from the cyber security point of view relies on an extensive off-line training with adequate data sets. The quality of these points determines the quality of on-line assessment.

Although there is room for improvements, this approach is a first step with good results in offering a better understanding and perspective of the impact that cyber-attacks can have on such a complex and interconnected system critical to the overall aspects of society.

REFERENCES

Anderson, P.M. and Fouad, A.A. (1977). *Power System Control and Stability.* The Iowa State University Press, volume 1.

Arghir, C., and Other (2016). On the steady-state behavior of a nonlinear power network model. *International Federation of Automatic Control (IFAC) Proceedings Volumes,* volume 49, Issue 22.

Barabanov, N., and Other (2016). Conditions for Almost Global Attractivity of a Synchronous Generator Connected to an Infinite Bus. *IEEE Transactions on Automatic Control*, volume 62, Issue 10.

Bitter, C., Elizondo, D.A., Watson, T., (2010). Application of Artificial Neural Networks and Related Techniques to Intrusion Detection. *IEEE World Congress on Computational Intelligence* (WCCI 2010), page number: 949 – 954.

Chaudhari, H.J., Mahindrakar, M. S., (2017). Feature Extraction of Malware Infected Files and Malicious Datasets, *International Journal of Innovative Research*

in Computer and Communication Engineering, volume 5, issue 6

Dabrowski, A. and Other (2017). Grid Shock: Coordinated Load-Changing Attacks on Power Grids - The Non-Smart Power Grid is Vulnerable to Cyber Attacks as Well. *Proceedings of the 33rd Annual Computer Security Applications Conference*, page numbers: 303-314.

de Silva, L. U. N., and Other (2015). Automatic governor for tie-line control: A teaching tool. *Moratuwa Engineering Research Conference (MERCon),* Moratuwa, Sri Lanka.

Dogaru, D.I., Dumitrache, I., (2017). Robustness of Power Systems in the Context of Cyber Attacks. *IEEE, 21st International Conference on Control Systems and Computer Science (CSCS)*, IEEE.

Dogaru, D.I., Dumitrache, I., (2018). Modelling the dynamic electrical system in the context of cyber-attacks. *Scientific Bulletin - Seria C: Inginerie Electrică şi Ştiinţa Calculatoarelor,* University Politehnica Bucharest.

Dumitrache, I., (2009) Distributed Control in Networked Systems, *Journal of Control Engineering and Applied Informatics*, volume 11, issue 3.

Dumitrache, I., Constantin, N., Stoica, O. (2013). Some challenges for the Cyber-Physical Energy Systems. *Proceedings of the 2nd IFAC workshop (ICPS-2013) on convergence of Information Technologies and Control Methods with Power Systems – IFAC Paper Plaza*, page numbers: 3-9.

Dumitrache, I. (2014). Intelligent Cyber-Energy-Systems. *Invited paper on ICTSCC-18th International Conference on System Theory, Control and Computing*.

Dumitrache, I., Dogaru, D.I., (2015). Smart Grid Overview: Infrastructure, Cyber–Physical Security and Challenges. *International Conference on Control Systems and Computer Science (CSCS),* IEEE.

Germond, A.J., Macabrey, N., and Other (2013). Application of Artificial Neural Networks to Load Forecasting. Neural Network Computing for the Electric Power Industry: *Proceedings of The 1992 INNSSummer Workshop*, page numbers: 165-171, Psychology Press.

Iftikhar, A., Azween, B.A., Alghamdi, A. S., (2009). Application of artificial neural network in detection of dos attacks. *Proceedings of the 2nd ACM international conference on Security of information and networks*, page numbers: 229–234.

Kalyani, S., Shanti Swarup, K. (2009). Study of Neural Network Models for Security Assessment in Power Systems. *International Journal of Research and Reviews in Applied Sciences*, volume 1, issue 2

Khadem, M., Dobrowolski,E., and Other (2013). Short-term Electric Load Forecasting Using Neural Networks. *Neural Network Computing for the Electric Power Industry: Proceedings of The 1992 INNSSummer Workshop*, page numbers: 173-178, Psychology Press.

Li, Y., and Other (2015). A Hybrid Malicious Code Detection Method based on Deep Learning. *International Journal of Security and Its Applications*, v\olume 9, No. 5 (2015), page numbers. 205-216

Lukic, Y.D., Stevens, C.R., and Other (2013). Application of A Real-Time Artificial Neural Network for Classifying Nuclear Power Plant TransientEvents. *Neural Network Computing for the Electric Power Industry: Proceedings Of The 1992 INNSSummer Workshop*, page numbers: 59-62, Psychology Press.

Mander, T. and Other (2007). Data object-based security for DNP3 over TCP/IP for increased utility commercial aspects security. *2007 IEEE power engineering society general meeting*, Florida, IEEE.

McCulloch, W. S., Pitts, W., (1943). A logical calculus of the ideas immanent in nervous activity. *The bulletin of mathematical biophysics*, volume 5, page numbers: 115–133.

Novosel, D., King, R.L., (2013). Intelligent Load Shedding. Neural Network Computing for the Electric Power Industry. *Proceedings of the 1992 INNSSummer Workshop*, page numbers: 107-1110, Psychology Press.

Samad, T., and Other (2013). Modeling And Identification with Neural Networks. *Neural Network Computing for the Electric Power Industry: Proceedings of the 1992 INNSSummer Workshop*, page numbers: 129-134, Psychology Press.

Semitekos, D., Avouris, N., (2002). A Machine Learning Toolkit for Power Systems Security Analysis. *Proc. IEEE PowerMed* 2002, Athens.

Swain, E.T., and Other (2006). The Application of Neural Networks to Electric Power Grid Simulation. *ICANN 2006: Artificial Neural Networks*, page numbers: 736-745.

Taha, A.F., (2015). Secure Estimation, Control and Optimization of Uncertain Cyber-Physical. *PhD thesis*, Purdue University.

Tomin, N.V., (2016). Machine Learning Techniques for Power System Security Assessment. *International Federation of Automatic Control (IFAC) Proceedings Volumes*, volume 49, issue 27, page number: 445-450.

Wu, C. H., (2009). Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks. *Expert Systems with Applications*, volume 36, page numbers: 4321–4330.

Wu, C. H., (2009). Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks. *Expert Systems with Applications*, volume 36, page numbers: 4321–4330.

Yousefian, R., Kamalasadan, S., (2017). *A Review of Neural Network Based Machine Learning Approaches for Rotor Angle Stability Control. Systems and Control; Neural and Evolutionary Computing*, Cornel University Library.

Zhang W., and Other (2011). Malicious web page detection based on online learning algorithm. *Proceedings of the International Conference on Machine Learning and Cybernetics (ICMLC)*, Publisher IEEE

Zhu, B., and Other (2011). A Taxonomy of Cyber Attacks on SCADA Systems. Internet of Things (iThings/CPSCom). *2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing*, IEEE.