Preliminary Approaches for improving the Smart Grid Cyber Security

Kathrin Reibelt, Ghada El Bez, Oliver Schneider, Jörg Matthes, Hubert B. Keller

Institut für Angewandte Informatik (IAI), Karlsruher Institut für Technologie (KIT), 76131 Karlsruhe, Deutschland
E-mails: kathrin.reibelt@kit.edu, ghada.elbez@kit.edu
Phone: +49(0)721 608-23973/ 28429

Abstract

The progressive digitization of the energy infrastructure in the course of the energy evolution requires reliable cybersecurity equipment that does not solely rely on access restrictions any more. For powerplants even frequently supplying fixes for vulnerabilities is not sufficient. One approach to repel attacks is the analysis of semantical and syntactical properties data of the communicated. For a fast detection of successful attacks the relations between parameters of control circuits can be evaluated. To ensure the security of our future energy system, the purpose of our work is to develop and establish independent, suitable monitoring systems within all components.

Keywords: cybersecurity, smartgrids, voulnerabilities, communication, control circuits

Introduction

For the energy evolution in Germany, the entire energy infrastructure is being rebuilt with power plants using renewable energy sources. A large number of small, decentralized power stations are replacing the large central power stations step by step. The fluctuating availability of renewable energy sources, as well as the increased energy demand due to mobility applications and the resulting higher fluctuations in demand, result in the need for much higher degrees of freedom in the network infrastructure. The large number of components requires intelligent remote control from a central position. The information network for control of those new plants, controllable transformers, prosumers etc. is called smart grid as it consists of smart devices. [3] Due to the high number of components interconnected in the smart grid and their spatial distribution, extensive protection against hacker attacks is required for such a control. In classical power plants, security is ensured primarily through the restriction of physical access or access rights. For high voltage transformers there is a dedicated optical fiber network. However, many examples from the past show that for smaller systems, far too often even the simplest access restrictions, e.g. password protection, are missing. But even if the usual protective measures have been taken, targeted attacks can rarely be repelled.

A current approach based on the concept of physical access restriction uses the so-called 'power-line' network in which the communication is transmitted directly via the power line. Although this network is not directly connected to the Internet, the power lines are accessible in every household by smart devices. Due to the large number of systems that would have to be integrated, however, threads from network vulnerabilities also encounters any possible independent, dedicated network.

Another approach based on informational access restriction uses cryptographic methods. A perfect implementation would lead to a huge increase of security in communication, as all connected devices can be identified and the data cannot be manipulated. Unfortunately there are always vulnerabilities caused by implementation faults and it does not protect from an attack that duplicates valid data or delays it in time.

It is therefore necessary to establish mechanisms which ensure the security of the system, regardless of access restrictions.

About Smart Grids

The main difference between conventional and smart grids is that the latter ones include cyber devices based on software functionality. The quick development of different technologies in the industrial field as well as in the home area increases the electricity requirement dramatically. Thus, use of various sources of energy, especially renewable ones is becoming a necessity considering new legislation and increasing energy consumption. Several factors allowed the development of smart grids over conventional energy systems. The main reasons of the advent of smart grids are described below.

- Providing a low-cost energy source thanks to the adjustment ability of a dynamic pricing system based on the consumption information,
- Respecting the imposed environmental regulations and standards,
- Renovating the aging infrastructures in traditional power grids,
- Resistance to disturbances and quick recovery from them [7].

In a nutshell, the main promise of smart grids is to provide a low-cost and an outage-free source of energy for the future [14].

Vulnerabilities in Smart Grids

The use of Information and Communication Technology (ICT) in smart grids (SG) allows the interaction between the different parties and stations involved in energy generation, transmission and distribution processes. Communication networks used in the modern SG may however raise different security concerns.

Smart grids are considered as critical infrastructures which makes ensuring security one of the major concerns. The presence of different vulnerabilities inherent in the structure of a smart grid make ensuring its security even more challenging. Some of the main weaknesses encountered while ensuring the security and the safety of the SG are summarized in the following points.

- The use of a massive number of devices including intelligent ones in the SG may result in the increase of the possible vulnerable points. Smart meters for instance can be maliciously used to indirectly influence the whole power plant.
- The coexistence of short-lived IT systems and legacy devices may result in incompatibilities and raise security concerns.
- An implicit trust is adopted for device-to-device communication also called machine to machine (M2M). This can affect the control system and make it vulnerable mainly to data spoofing as the state of one device alters the functionality of another [1].
- The growth of the number of stakeholders in modern smart grids leads to new threats such as insider attacks.
- The adaption of network protocols found in general computer systems to power plants implies the same threats encountered in the former systems.
- Almost all usual software contains weaks or faults in the implementation that lead to significant vulnerabilities [6].

Countermeasures against Smart Grids Cyber Threats

Traditional solutions against cyber-attacks in smart grids were adapted from the ICT field such as access restrictions. However, those methods are not adequate for application to the smart grid due to its specificities. In fact, in a critical infrastructure such as a smart grid, availability, integrity and certain levels of confidentiality are required in this order of priority [9].

To harden the cybersecurity of the modern energy systems against attacks several techniques ranging from firewalls to intrusion detection and prevention tools are used. Industrial protocols used in smart grids such as Modbus TCP or DNP3, for the most do not have integrated network security solutions. Attacks such as DoS or DDoS, MIM (Man-in-the-middle) can have disastrous consequences as shown by the reported accidents in the few last years.

Consistent work on developing intrusion detection systems has been done. High rates of intrusion detection with low rates of false positive were reached. Jyothi et al. in [5] claim reaching a detection rate of DDoS attacks of 99.8 % and a false alarm rate of 0 % using BRAIN, a behaviour based intrusion detection tool that uses an algorithm that combines low-level hardware events, network statistics and application parameters. Many researchers claim reaching such high rate of detection, however they rarely consider latency detection [10]. In fact, time is a decisive factor in the case of a cyber-attack affecting a critical infrastructure such as a SG. If an intrusion detection system has a high detection latency, the target could be damaged before the intrusion is detected.

An approach that enables the detection of intrusions within a reasonable time in a first stage and their prevention in a second one is highly needed to secure the network communication in smart grids. The semantic and syntactic checking of the data transmitted within the network of the smart grid is a promising approach to protect this critical infrastructure mainly against availability attacks. Further work will focus on developing solutions to reach this goal.

Cybersecurity of energy systems, a model-based approach

The detection of attacks requires in most cases prior knowledge of the weak points of the computer system or knowledge of the behavior of the malicious software. In the current systems new vulnerabilities are constantly being discovered, for which the signatures for the detection and the necessary fixes are provided in the form of updates. However, for energy infrastructure as a critical infrastructure, these updates are often applied only after years, because every change to the system has to be validated by extensive tests [4].

In order to recognize a successful attack regardless of its signature knowledge about the interoperation of the components in the affected system is necessary.

The plants are equipped with a standard system that detects states which could cause damage to the plant and trigger an emergency shutdown. The usual protection systems, as they are used in most facilities, define independent expectation intervals for all measured values. If a value exceeds such an interval, the system is switched off. The exact deviation, i.e. direction and magnitude, enables conclusions in cause of a known malfunction but lacks information to classify an unknown malfunction [8, 13]. Protection against artificial attacks is rarely possible because the independence of the intervals provides sufficient margins for manipulations that will not be detected. Even without an attack some plants were damaged in the past despite those protection systems [12]. For the detection, the preprocessed data from smart sensors are used, so the sensors themselves can be manipulated. Manipulations which do not lead to a damage, such as the reduction of the requested power, are not recognized by these systems at all.

In addition, these security systems enable new possibilities of attack. In order to take the plant off the grid, only a prohibited operating state has to be emulated or physically reached by the attacker. Also this is no problem for a single plant, it is risky for the power system as all components are connected and accessible with standardized communication. Thus a specific manipulation could apply to multiple plants and therefore take entire groups of plants off the grid.

The idea considered in the following is to introduce an independent monitoring system, which checks the control circuits for invalid behaviour and in future systems validates the measured system states with a minimum number of additional, reliable measurements. The correlations between the different control and measured variables as well as their derivatives can be condensed from the existing models of the plants.

For a quick fix of the malfunction, additional information about the component which is most likely the tampered one, is helpful. In addition to the fast recommissioning of the affected plant function, this knowledge could also be used to test identical components in other systems. Therefore the aim is a classification of the malfunctions, which is independent from the knowledge of the signature of the specific malfunction.

The following methods are investigated on the Simulink model of a wind turbine [2]. The actuating variable is the requested power from which the control calculates a set point for the pitch angle depending on the measured supplied power. The wind is then the mediating parameter, and changes of the wind can be considered a disturbance that affects the system. The requested power is 3 MW in the unmanipulated case.

A method presently used in industrial plants is the simulation during runtime with the measured conditions. The values calculated by the simulation can either be compared directly to the measured ones or individual features can be compared. Since the behavior of the systems is described much more precisely here, this approach is more suitable for the detection of an attack than in the comparison with intervals. As for the intervals the deviations between measurements and simulated values provide information on the causes of the malfunction, in case of a known pattern. A major issue is that the simulation can take very long if the system behavior is mapped accurately. Thus, for a real-time application simplifications may be necessary [8, 13].

In the example (Fig. 1), the pitch angle is manipulated to 0°, implying the maximum energy transfer. The measured curve can be seen in red. The figure shows the output values by the pitch control (not the manipulated true pitch value of 0°). The wind speed is increasing continuously. In order to reduce the measured power, the control attempts to increase the pitch more and more. As the true pitch remains at 0° the generator speed increases. The efficiency of the generator depends on the speed as it feeds to a grid with rotating current of a certain frequency. So the reached speed finally leads to decreasing power and the protection system interrupts the operation after 6.6 s because of low Voltage, the trace ends prematurely. In parallel, the expected behavior of the unmanipulated system is simulated with a model, shown in blue. Here the power is regulated at 3 MW by increasing the pitch angle as long as the wind exceeds the minimum speed required for nominal power.

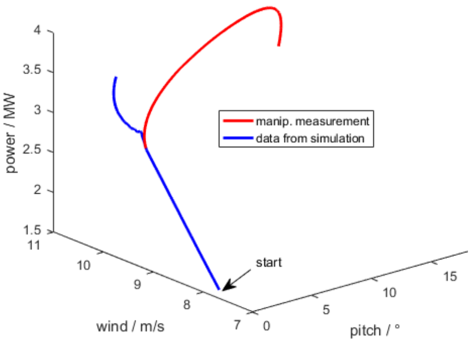

Fig. 1: Trace from Simulink simulation of a wind turbine and trace of parallel simulation during runtime. Manipulation: pitchangle kept at 0°.

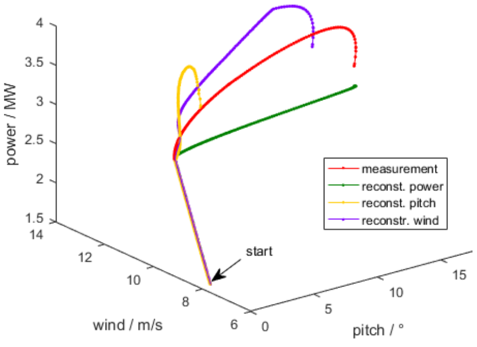

Fig. 2: Trace from Simulink simulation of a wind turbine and statical reconstructions of any parameter on the others. Manipulation: pitchangle kept at 0°.

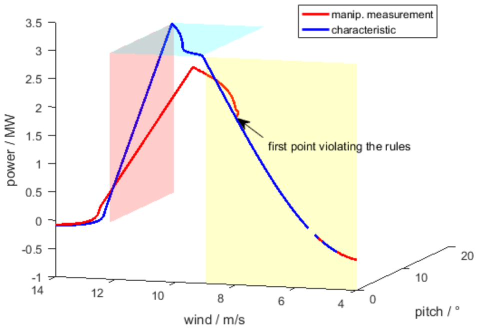

Fig. 3: Static characteristics (usual characteristic and one manipulated) from Simulink simulation of a wind turbine and regions with similar behavior. Manipulation: reduced power request.

To improve the speed of the analysis, the static interrelationship of observables involved in one control loop can be used as simplification. Such possible redundancies in the system can be identified by the model [11]. For a group of observables that have interrelationships, each variable is reconstructed from the others. If the reconstructions differ significantly from the measurement this indicates a manipulation, in case of almost bijective dependencies. In the next example (Fig. 2), the pitch angle is manipulated to 0°, as in the first example. All reconstructed traces differ obviously from the measured one. A manipulation is suggested. A helpful supplement to indentify the manipulated parameter would be the safe, secure and independent measurement of the most meaningful parameters.

Another possibility to detect manipulations is to simplify the system by dividing it into regions with similar behavior. Rules are defined describing the behavior in each of these regions. The information which rules are broken allows conclusions on possible causes. Dependencies between the rules are identified. For example, the break of a certain rule results in the breaking of a second rule, whereas it does not result from the second rule. So the additional information which regions were entered is required. If this method shows an anomaly, it can be evaluated, if the suspicious section of trace matches the rules of the next region.

The third example (Fig.3) shows an unmanipulated characteristic in blue, which lies in the planes. The different planes mark regions of common rules. In the yellow region, the pitch angle, as well as its derivative, must be at 0, the wind speed is between 5 m/s and 9 m/s, and a positive derivative of the wind is associated with a positive derivative of the power. Correspondingly, a negative derivative of the wind is accompanied by a negative derivative of the power and a constant wind speed with a constant power. For the recording of the red line, the pitch control uses a requested power manipulated to a lower value. Both curves are static characteristics. For dynamic traces, slight deviations from the characteristic curves occur which, however, have no influence on the fulfillment of the rules. It can be seen that the curves in the yellow region agrees with the rules for the most part. Only in the upper range a deviation occurs at power and pitch angle. In the blue and red regions, deviations occur with pitch angle and power.

In order to get additional information, the curve from the first point that violates the rules in the yellow region is shifted so that it lies on the transition to the blue region. The shifted curve now fulfills the rules of the blue range. This leads to the conclusion that the wind turbine behaves normally, it only depends on a wrong target power. The displacement of the curve in the direction of a lower wind speed is a logical consequence of the displacement to a lower power and therefore only confirms the conclusion. A wrong measurement of the wind force would only require a shift on the wind scale.

Conclusion

The methods introduced are meant to ensure the integrity of communication and control loops in the energy system of the future. On such methods a diagnostic system has to be developed that should be realized as an embedded system with very limited communication possibilities, in order to ensure the future protection of power plants and automated industrial plants.

References

[1] Aloul, Fadi and Al-Ali, AR and Al-Dalky, Rami and Al-Mardini, Mamoun and El-Hajj, Wassim. “Smart grid security: Threats, vulnerabilities and solutions.” *International Journal of Smart Grid and Clean Energy* 2012: 1-6.

[2] Gagnon, Richard (2004): „Wind Farm (IG)“, https://de.mathworks.com/examples/simpower/mw/sps_product-power_wind_ig-wind-farm-ig (2017-2-21).

[3] Hagenmeyer, Veit; Cakmak, Hüseyin Kemal; Düpmeier, Clemens; Faulwasser, Timm; Isele, Jörg; Keller, Hubert B.; Kohlhepp, Peter; Kühnapfel, Uwe; Stucky, Uwe; Waczowicz, Simon; Mikut, Ralf: "Information and communication technology in energy lab 2.0: Smart energies system simulation and control center with an open-street-map-based power flow simulation example" in Energy Technology, Vol. 4, pp. 145-162, ISSN 2194-42882194-4288, DOI 10.1002/ente.201500304, 2016.

[4] International Atomic Energy Agency Vienna (2011): “Computer security at nuclear facilities”, IAEA Nuclear Security Series No. 17, Technical Guidance Reference Manual, ISBN 978–92–0–120110–2.

[5] Jyothi, Vinayaka and Wang, Xueyang and Addepalli, Sateesh K and Karri, Ramesh. “Brain: Behavior based adaptive intrusion detection in networks: Using hardware performance counters to detect DDoS attacks.” *VLSI Design and 2016 15th International Conference on Embedded Systems (VLSID), 2016 29th International Conference on*. IEEE, 2016. 587-588.

[6] Keller, H. B.; Schneider, O.; Matthes, J.; Hagenmeyer, V.: Zuverlässige und sichere Software offener Automatisierungssysteme der Zukunft – Herausforderungen und Lösungswege. *at – Automatisierungstechnik* 2016; 64(12), S. 930–947.

[7] Kush, Nishchal and Foo, Ernest and Ahmed, Ejaz and Ahmed, Irfan and Clark, Andrew. “Gap analysis of intrusion detection in smart grids.” *Proceedings of the 2nd International Cyber Resilience Conference.* 2011. 38-46.

[8] Lichtenberg, G. (2011): „Methoden der modellbasierten Fehlerdiagnose“, http://www.modqs.de/fileadmin/user_upload/Workshops/Vortraege_2011/ModQS-Workshop-2011-Lichtenberg.pdf (2016-10-19).

[9] Liu, Jing and Xiao, Yang and Li, Shuhui and Liang, Wei and Chen, CL Philip. “Cyber security and privacy issues in smart grids.” *IEEE Communications Surveys & Tutorials* (2012): 981-997.

[10] Mitchell, Robert and Chen, Ing-Ray. “A survey of intrusion detection techniques for cyber-physical systems.” *ACM Computing Surveys (CSUR)* (2014): 55.

[11] North Carolina State University, University of Ottawa (2003): „Introduction to Data Reconciliation“, http://www.polymtl.ca/namp/docweb/Modules_Web/M11_Tier1_Chap1-3.pdf (2016-10-18).

[12] Schultz, Stefan (2017): „Das Geheimnis der umgeknickten Windräder“, http://www.spiegel.de/wirtschaft/unternehmen/windkraft-traege-rotorregler-fuehrten-laut-analyse-zu-mysterioeser-havarie-serie-a-1137530.html (2017-3-10).

[13] Schwenken, U. (2006): „Eine Methode zur Fehlerbewertung und zur adaptiven Motorleistungsbegrenzung auf der Basis einer modellbasierten Diagnose am Beispiel eines PKW-Kühlsystems“, Dissertation, Ruhr-Universität Bochum.

[14] Sorebo, Gilbert N and Echols, Michael C. Smart grid security: *an end-to-end view of security in the new electrical grid*. CRC Press, 2011.