https://doi.org/10.5281/zenodo.10449604

A REVIEW OF CYBER THREAT DETECTION METHODS IN POWER SYSTEMS WITH INTRUSION STATE ESTIMATION PROGRAM

Mustafa Eydyany
Energy Security and Sustainable Energy Institute, Modarres 4, P.C.: 9188874391, Mashhad, Iran
eidiani@ijesse.net

Abstract. The digitalization of the power system has increased information and online control of this network, but it has created a new threat in cyber security. Hackers' blackouts of the Ukrainian power grid and the Stuxnet worm show the possibility of widespread and integrated attacks on the power system. There are many fault detection mechanisms in the power system that rely on entering the wrong data. It is easy for the state estimation program to distinguish the incorrect data from the correct data. The problem begins with the fact that these error detection programs may fail when false information is consistently present. The purpose of this article is to provide a comprehensive review of various references on this topic. For clarity, the article is divided into two separate sections, cyber-attacks and state estimation.

Keywords: State estimation, Energy management system, Power system cyber security

چکیده: کنترل آنلاین و حجم اطلاعات سیستم قدرت به دلیل دیجیتالی شدن افزایش یافته است اما تهدید جدیدی در امنیت سایبری نیز ایجاد کرده است. خاموشی شبکه برق اوکراین و تولید کرم استاکس نت توسط هکرها، افزایش احتمال حملات گسترده و یکپارچه به سیستم قدرت را نشان می‌دهد. مکانیسم‌های تشخیص عیب بسیاری در سیستم قدرت وجود دارد که بر روی وارد کردن اطلاعات اشتباه تکیه می‌کنند. برای برنامه تخمین حالت، تشخیص داده‌های نادرست از داده‌های صحیح آسان است. مشکل وقتی شروع می‌شود که این برنامه‌های تشخیص خطا با ورود اطلاعات نادرست به طور مداوم، شکست بخورند. هدف از این مقاله بررسی جامع منابع مختلف در این زمینه است. برای وضوح بیشتر، مقاله به دو بخش حملات سایبری و تخمین حالت تقسیم شده است.

کلمات کلیدی: تخمین حالت، سیستم مدیریت انرژی، امنیت سایبری سیستم قدرت

1- An introduction to cyber-attacks in the power system

Among the applications of digital development and automation in power systems is the use of energy management systems (EMS). Information and communication technology (ICT) infrastructure, phasor measurement units (PMU), state estimation programs (SE), automated generation control (AGC), and supervisory control and data acquisition (SCADA) have all been developed as a result of the digitization of the power system. Cyber security threats have been exposed to the power system due to the vulnerability of ICT infrastructure. Because SCADA systems use legacy technology, they are popular targets for adversaries [1].

SCADA network protocols, such as Modbus protocol, Distribution Network Protocol (DNP3), IEC 60870-5, and IEC 61850, do not provide strong network security [2]. Furthermore, SCADA systems are increasingly connected to corporate networks and the Internet, increasing the potential for malicious cyberattacks. Hackers can use control centers, substations, or remote access points to hack into corporate or Internet networks.

Hackers can disrupt the synchronicity of SCADA protocols, compromise communication availability, or even control or change sensors and actuators when they penetrate a SCADA network. An attack on a SCADA system can cause incorrect operation, affect power system reliability and economics, and even cause cascading outages [3].

The following section provides two examples of cyber risks caused by deliberate malware and adversary attacks. Stuxnet and the Ukrainian network shutdown. According to 1-1, the Stuxnet worm attack has a surprising combination of advanced skills, internal system knowledge, extensive attack resources, and

Corresponding author's e-mail: eidiani@ijesse.net

excellent stealth capabilities. In the SCADA system, this malware contains code for manipulating sensor measurements and control signals without identifying the attacker. In (1-1), attackers can perform the long reconnaissance operations necessary to master the system and execute a multi-site attack that is highly coordinated [4].

According to the National Institute of Standards and Technology (NIST), protecting ICT infrastructure involves five functions: identifying, protecting, discovering, responding, and recovering. Bad data detection (BDD) detectors and SCADA systems are used to filter possible wrong measurements due to defective sensors [5]. BDD is essentially a static detection scheme since it only captures a snapshot of the steady-state system's trajectory. This method can detect some basic attacks, but it may fail in the presence of hidden multivariate attacks with carefully synthesized false data. The detection of such covert attacks has been proposed by many methods. There have been several statistical methods proposed and discussed in [6], such as sequential detection utilizing a Cumulative Sum algorithm (CUSUM).

1-1- Two examples about cyber risks

This section presents two examples of malicious malware and enemy attacks that pose cyber risks. Stuxnet and the Ukrainian network shutdown.

1-1-1- As far as industrial control systems (ICSs), such as SCADA networks and critical power grid infrastructure go, Stuxnet is the most sophisticated and practical malware. Several countries, including Iran, India, and Indonesia, are targeted by this malicious computer worm. In order to disrupt Iran's nuclear program, the primary target was its uranium enrichment facilities. Stuxnet is believed to have infected many personal computers and damaged thousands of industrial facilities [8].

The main features of the Stuxnet worm are as follows [9]:

• Highly selective targeting, from vulnerable PCs to programmable PLCs.

• Four "zero-day attacks"[1], an unusually high number.

• Very detailed knowledge of PLCs and ICSs.

• Using a "Windows rootkit"[2] to conceal the owner of the computer.

• A lot of attack resources and a high level of effort.

• Long standby time and powerful auto-update capabilities.

• A large number of infected hosts and organizations.

1-1-2- Hackers cause the first blackout of Ukraine in 2015

On December 23, 2015, hackers caused the first blackout in Ukraine. There were several technical components to these cyberattacks [10]:

• Identification of long-term victim networks for learning about the environment and systems

•Phishing emails used to compromise corporate networks with malware "Black Energy 3"[3].

[1] Zero-day attacks (zero-day exploits) refer to vulnerabilities that are new to zero-day. Other parties or malicious actors may discover a vulnerability and wait to exploit it strategically or sell it to those who can exploit it. A zero-day vulnerability is extremely dangerous since no action has been taken to fix or protect it.

[2] Rootkits are software programs that take control of a computer system. As a result of this type of attack, the system user will not notice the presence of the rootkit and hacker will be able to change all computer settings without the user's knowledge.

[3] The BlackEnergy malware was first spotted in 2007 as an HTTP-based toolkit that executed distributed attacks with bots. "Black Energy 2" emerged in 2010 with capabilities beyond DDoS. Black Energy 3 was also equipped with a variety of plugins in 2014. Russian group Sandworm (aka Voodoo Bear) is credited with using "black energy". An attachment to an email, consisting of a Word document or PowerPoint presentation, targets victims by luring them to click on what appears to be a legitimate file.

- Remotely shutting down substations by hacking the SCADA network
- SCADA infrastructure disruptions such as modems, RTUs, etc[4].
- Use KillDisk[5] Corrected to destroy server and mainframe master boot records.
- Compromise of outage reports through TDoS attacks[6].

2- An introduction to state estimation

State estimation (SE) in modern energy management system (EMS) is an example of the dependence between physical power system and ICT infrastructure . The operator can estimate the state of the system based on SCADA's load distribution measurements. Today, SE is an integral tool in EMS for Contingency analysis (CA), security-constrained optimal power flow (SC-OPF), and price calculation and ATC determination algorithms. The critical nature of SE highlights the importance of its accuracy and security for power system operation. However, the SCADA system is vulnerable to a large number of security threats [11].

In numerous references, false data injection (FDI) attacks have been studied as a typical class of data integration attacks. An accurate data fusion attack can inject synthesized false data (FDI) into a number of SCADA measurements. This multivariate attack bypasses SE's BDD mechanism by changing several measurements in concert [12]. As a result, the hacker has full knowledge of the system model's topology and parameters. As well as manipulating multiple measurements, it can also hide from detection schemes and achieve specific objectives with enough attack resources. Cyberattacks against SCADA networks in power systems are characterized by these capabilities.

Due to the fact that state estimation (SE) is based on the load flow model and can be used by many tools in EMS to identify failures, failure estimates can influence a number of control mechanisms. The number of resources needed to change certain measurements and remain stealthy is usually measured by calculating the amount of resources an adversary has at his disposal [12].

Usually, the concept of security index is introduced with the following optimization program formulation, where alfa represents the security index and (f) represents the FDI attack [5].

$$\alpha = \min \sqrt[p]{\sum_{i=1}^{n} |f_i|^p}, \; s.t. : f \in S_1, f \in S_2 \tag{1}$$

A set of attack vectors (f), a list of the attacker's goals (S1), and a list of methods for hiding from potential detectors (S2) are included in equation (1) [5]. The enemy must coordinate a significant amount of resources to attack alfa if it is large. Some measurements become critical when alpha is small, because they require less deviation to change covertly. Thus, power systems with a lower security index are more vulnerable to attacks.

It is also important to point out that in most of the reviewed papers in the literature, adversaries are still assumed to have complete knowledge of the system, whereas an attacker may obtain a perturbed system model if he analyzes an old or estimated model obtained by an attacker [13].

---

[4] A Remote Terminal Unit (RTU) is an electronic device controlled by a microprocessor that receives and transmits information about existing devices and equipment. Connecting the RTU with a control system or SCADA allows it to transmit telemetry data and receive control information from the control center. The RTU receives analog and digital signals from the equipment and transmits them to the central control system. It is possible to monitor and control devices and equipment using RTU.

[5] KillDisk is a powerful and new tool for permanently deleting system data. It allows the user to delete his digital information on the hard drive, flash memory, memory card, etc. in a way that cannot be recovered by any recovery software.

[6] TDoS or "Telephony Denial of Service" refers to the attempt to block incoming or outgoing calls from a telephone system. There is no empty telephone line when an attacker successfully occupies all available telephone resources.

2-1-Reviewing the references of using state estimation

Different aspects of cyber risk assessment are the focus of FDI attacks against SE, according to research. An example of a vulnerability analysis would be an analysis of the impact of an attack, and the development of a "risk mitigation" plan. "Risk mitigation" planning involves identifying options and taking actions to reduce threats and increase opportunities. FDI attacks such as hidden multivariate attacks, first demonstrated in [12], can disrupt state estimation (SE) in SCADA networks without raising alarms in BDD. Furthermore, state estimation can also be vulnerable to hidden multivariate attacks [12] if the attacker manipulates certain measurements and remains hidden from the BDD scheme.

The structural vulnerability of power systems to failures or intentionally attacked is also quantified with sophisticated techniques as part of the broader analysis of vulnerability. In [14], a new central index for assessing network vulnerability is introduced as a major subclass of topological methods. In [15], topological and operational vulnerabilities are considered in a cascaded fault graph approach.

A corrupt SE can contaminate other control measures in EMS and force operators to make destructive decisions if it is fed into any of the other applications. The authors analyze estimation errors caused by multivariate stealth attacks in [16]. In these papers, the authors demonstrate that error rates can be high even when only a small number of measurements are compromised. As shown in reference [3], the price of nodes in the electricity market can be used to determine the economic impact of multivariate attacks against SE. As shown in this reference, the attacker can profit economically or cause operational costs. The physical impact of such attacks with the attacker's goal of overloading the lines has recently been studied in reference [17]. Risk mitigation schemes have been proposed to protect certain measurements from hostile data injection, to defend against multivariate stealth attacks, and to improve the BDD algorithm. [6] describes the well-known Cumulative Sum Algorithm (CUSUM) that is used to detect sequentially (or at the fastest possible time) covert attacks.

Synchrophasor data and other predicted information were used in reference [7]. Mitigation schemes at the network and application layers, such as data protection, and multipath routing, authentication, have proven to reduce the vulnerability of power systems. Almost all of the above research assumes that the adversary has full knowledge of the power network, including its topology and parameters. Nevertheless, adversaries rarely execute attacks with full knowledge of system models, and data about system models is usually protected. According to Reference [18], FDI attacks can also be performed on networks with incomplete information. In certain circumstances, the attacker can still remain hidden from the system even if he knows the local information (transmission line parameters and topology) of the attack area. FDI attacks based on incomplete AC state estimation were also investigated in reference [19]. An attacker with limited knowledge may also have misinformation about the power system network [13]. Such FDI attacks may be detected by the BDD mechanism, while topology detection capacity or parameter errors are closely related to detection capability [5].

By using learning methods such as independent component analysis (ICA) and subspace estimation, the adversary can also infer the necessary network information for all the above limited knowledge cases [20]. DIgSILENT PowerFactory software has been used in most of the research, as explained below.

3- The reason for using DIgSILENT PowerFactory

Power system dynamics models play an important role in the effectiveness of the presented model-based methods. The generated models of complex power systems are, however, mostly non-linear and high-dimensional. In addition, an accurate real-time model of a power system is not always available. Whenever a complete model of a power plant is unavailable, high-fidelity simulators (e.g., DIgSILENT) are necessary to accurately describe the system. The simulators provide additional insight into the behavior of networks.

It is possible to simulate a numerical model in the simulators. In contrast, mathematical models that specify physical laws in the form of differential equations and dynamic systems (such as Matlab) are

simplified at the expense of software efficiency. A mismatch always exists between the simulation model and the mathematical model of the power plant. Since such a model mismatch always exists, implementing diagnostic tools based on the real system or its exact simulation is trivial. In most recent references [21-23], model-based detectors are implemented using high-quality simulators (such as DIgSILENT). This situation fills the gap between data-driven and model-based approaches, resulting in a model-based approach for the implementation of the diagnostic tool with the help of new data.

Furthermore, this software is used by hundreds of regional electricity companies, distribution companies, and consulting companies in Iran and abroad. Voltage, current, power, tap transformers, and network switch status are determined using offline and online state estimation programs. All other outputs will be overridden if this information is changed.

4 - Conclusion

In spite of the advantages of digitization and automation in the power system, cyber-attacks are a significant threat to the system and indicate unsafe use of this technology. Both complete and incomplete information can be used by hackers to achieve their goals. This paper examines the weaknesses of the state estimation program when full network information is available to change the information.

Reference

[1] S. Gorman, "Electricity grid in US penetrated by spies", The Wall Street Journal, Vol. 8, 8 April 2009.

[2] INL/EXT-10-18381. "Vulnerability Analysis of Energy Delivery Control Systems", Idaho National Laboratory Idaho Falls, Idaho 83415, Sep. 2011.

[3] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations", IEEE Transactions on Smart Grid, Vol. 2, No. 4, pp. 659–666, Dec. 2011.

[4] D. Case, Analysis of the cyber attack on the Ukrainian power grid, Mar. 2016. Available at https://media . kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[5] A. Teixeira, S. Amin, H. Sandberg, KH Johansson, and SS Sastry, "Cybersecurity analysis of state estimators in electric power systems", 49th IEEE Conference on Decision and Control, pp. 5991–5998, 2010.

[6] S. Li, Y. Yılmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids", IEEE Transactions on Smart Grid, vol. 6, no. 6, pp. 2725–2735, 2015.

[7] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," IEEE Transactions on Smart Grid, vol. 9, pp. 1636–1646, May 2018.

[8] B. Kesler, "The vulnerability of nuclear facilities to cyber attack", Strategic Insights, vol. 10, no. 1, pp. 15–25, 2011.

[9] TM Chen and S. Abu-Nimeh, "Lessons from stuxnet", Computer, vol. 44, no. 4, pp. 91–93, 2011.

[10] G. Liang, SR Weller, J. Zhao, F. Luo, and ZY Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks", IEEE Transactions on Power Systems, vol. 32, pp. 3317–3318, July 2017.

[11] M. Eidiani, H. Zeynal and Z. Zakaria , "Development of Online Dynamic ATC Calculation Integrating State Estimation," 2022 IEEE International Conference in Power Engineering Application (ICPEA), 2022, pp. 1-5, doi : 10.1109/ICPEA53519.2022.9744694.

[12] A. Teixeira, KC Sou, H. Sandberg, and KH Johansson, "Secure control systems: A quantitative risk management approach", IEEE Control Systems, vol. 35, no. 1, pp. 24–45, 2015.

[13] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, "Data attacks on power system state estimation: limited adversarial knowledge vs. limited attack resources", 43rd Annual Conference of the IEEE Industrial Electronics Society, pp. 4313–4318, Oct. 2017.

[14] A. Dwivedi and X. Yu, "A maximum-flow-based complex network approach for power system vulnerability analysis", IEEE Transactions on Industrial Informatics, vol. 9, pp. 81–88, Feb. 2013.

[15] X. Wei, J. Zhao, T. Huang, and E. Bompard, "A novel cascading faults graph based transmission network vulnerability assessment method", IEEE transactions on power systems, vol. 33, no. 3, pp. 2995–3000, 2017.

[16] O. Kosut, L. Jia, RJ Thomas, and L. Tong, "Malicious data attacks on the smart grid", IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 645–658, 2011.

[17] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation", IEEE Transactions on Power Systems, vol. 31, pp. 3864–3872, Sept. 2016.

[18] X. Liu, Z. Bao, D. Lu, and Z. Li, “Modeling of local false data injection attacks with reduced network information”, IEEE Transactions on Smart Grid, vol. 6, no. 4, pp. 1686–1696, 2015.

[19] X. Liu and Z. Li, "False data attacks against AC state estimation with incomplete network information," IEEE Transactions on Smart Grid, vol. 8, pp. 2239–2248, Sept. 2017.

[20] J. Kim, L. Tong, and RJ Thomas, "Data framing attack on state estimation", IEEE Journal on Selected Areas in Communications, vol. 32, July 2014.

[21] P. Kaikai, Pan, Towards Cyber-secure Intelligent Electrical Power Grids: Vulnerability Analysis and Attack Detection. https://doi.org/10.4233/uuid:4b4f9f96-237e-421b-82f4-97b1393ae507 , 2020.

[22] M. Eidiani, "A rapid state estimation method for calculating transmission capacity despite cyber security concerns", IET Gener . Transm . Distrib . 1–9 (2023). https://doi.org/10.1049/gtd2.12747

[23] M. Eidiani, H. Zeynal and Z. Zakaria , "An Efficient Method for Available Transfer Capability Calculation Considering Cyber-Attacks in Power Systems," 2023 IEEE 3rd International Conference in Power Engineering Applications (ICPEA), Putrajaya, Malaysia, 2023, pp. 127-130, doi : 10.1109/ICPEA56918.2023.10093168.