Stealthy Rootkit Attacks on Cyber-Physical Microgrids

Suman Rath
V. S. S. University of Technology
Burla, India

Ioannis Zografopoulos
KAUST
Thuwal, Saudi Arabia

Charalambos Konstantinou
KAUST
Thuwal, Saudi Arabia

ABSTRACT

Cyber-physical microgrids hold the key to a carbon-neutral power sector since they enable renewable and distributed energy resource integration, can alleviate overloaded distribution systems, and provide economic energy by generating and consuming power locally. The utilization of cyber-physical assets such as controllers, IoT sensors and actuators, and communication devices can enhance the stability and improve the control of microgrids. However, such assets, if maliciously operated, can become attack entry points and jeopardize the grid operation. Blind and uncoordinated cyber-attacks can be identified by existing security measures overcoming potential operational disruptions. However, rootkit attacks can stay hidden within cyber-physical systems and leverage system information to mask their presence. Rootkit detection is a strenuous process and requires advanced security methods due to their sophisticated operation. A careful analysis of possible rootkit target locations and their exploitation techniques is necessary to design effective threat detection and mitigation mechanisms. This paper discusses the cyber kill chain of a rootkit which can simultaneously deploy itself at multiple locations in a microgrid in a coordinated and stealthy way in order to maximize the impact on power system operations. The rootkit leverages system measurements to hide its presence and its attack impact from the detection mechanisms.

CCS CONCEPTS

• **Security and privacy** → *Malware and its mitigation*; • **Hardware** → *Smart grid*.

KEYWORDS

Rootkit, cyber-physical microgrid, coordinated cyber manipulation, intelligent malware, data-driven prediction, virtual twin.

ACM Reference Format:
Suman Rath, Ioannis Zografopoulos, and Charalambos Konstantinou. 2021. Stealthy Rootkit Attacks on Cyber-Physical Microgrids. In *The Twelfth ACM International Conference on Future Energy Systems (e-Energy '21), June 28-July 2, 2021, Virtual Event, Italy*. ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3447555.3466576

1 INTRODUCTION

Microgrids foster the penetration of renewable energy sources which are environment-friendly alternatives to energy sources such as coal-fired thermal power plants. Closely coupled cyber and physical layers guarantee the increased flexibility and robust operation of microgrid deployments. The information and communication cyber layer receives inputs from sensors and issues control commands to elements in the physical layer. As a result, malicious adversaries can exploit cyber layer vulnerabilities (e.g., insecure communications protocols) to port their attacks impacting the control and stability of cyber-physical microgrids [4]. Attacks capable of manipulating sensor measurements can have significant impact on such systems (e.g., blackouts, brownouts, human safety, equipment damage, etc.).

In literature, many researchers have aimed to address the aforementioned issue by developing various cyber-attack use cases and their exploitation techniques, along with methodologies to detect and mitigate them [5]. Rootkits represent a class of malware which can intelligently hide their presence inside their targets [1]. They can eavesdrop system data/measurements and allow attackers to collect real-time system information via remotely accessible connection links. Adversaries can exploit these connections to port malicious commands, manipulate the infected host device(s), and stealthily control their operation.

Microgrid-based rootkit attack studies are of paramount importance for the design and implementation of potent detection and mitigation strategies. This paper presents a potential rootkit attack path after the successful installation of the malware at multiple vulnerable locations inside the microgrid. It also delineates different approaches that rootkits can utilize to conceal their presence (during the system information aggregation phase) and disguise their attack impact overcoming existing security fortifications.

2 ATTACK MODEL

Threat model discussion: Our threat modeling assumes that the rootkit, and the attacker, can access and modify sensors measurements and controller strategies at different levels and locations within the microgrid. Furthermore, the rootkit, by collecting sufficient system information can anticipate the microgrid state trajectories, and thus disguise its operation as well as the attack impact while remaining undetected by the system operators.

This paper proposes the concept of a rootkit attack which collects information (from the physical layer) to hide its presence inside the cyber-physical microgrid system. A microgrid model infected with the rootkit is shown in Figure 1. Once the rootkit gains access to various microgrid elements (e.g., controllers, actuators, etc.), it starts eavesdropping on the system information. Such data could include vital state parameters leveraged to build a virtual data-driven model – similar to a digital twin – of the entire microgrid system. The granularity of the virtual replica depends on the attacker's objectives and capabilities as well as the available resources. This virtual model is then employed to predict future system states and control operations. The attacker uses the predicted values of the virtual microgrid model to bypass security mechanism and remain

e-Energy '21, June 28-July 2, 2021, Virtual Event, Italy

ACM ISBN 978-1-4503-8333-2/21/06…$15.00
https://doi.org/10.1145/3447555.3466576

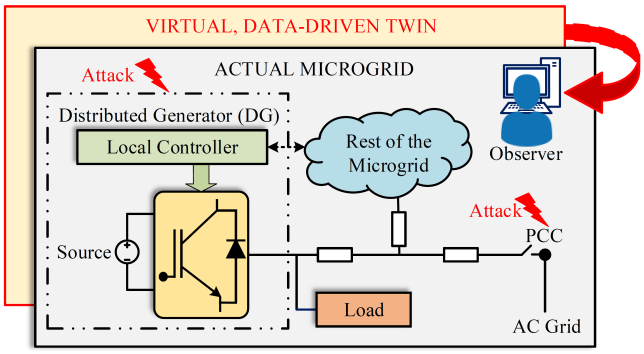

Figure 1: Proposed Attack Model.

undetected by system operators at multiple levels. The proposed attack aims to create gradual changes at the local Distributed Generation (DG) level whose effects can propagate through grid devices (e.g., controllers, smart inverters, smart meters, etc.) impacting the overall power system. The changes can range from minor alterations, like voltage bias injections with minor effects on system performance, to noise additions in sensor measurements which can generate erroneous control inputs to grid devices (e.g., inverters) affecting the power generation, voltage stability, and introducing harmonic frequencies [2, 5]. Although such perturbations might be small in magnitude to remain undetected (less than the security detection thresholds), their impact can increase over prolonged periods of time and threaten the nominal system operation.

Rootkit attack methodology: The malware is able to intelligently initiate the coordinated manipulation of power electronic converters at both the DG level as well as at the Point of Common Coupling (PCC) to maximize its impact. For instance, the manipulation of sensor measurements at the PCC level can be used to trigger false alarms (e.g., indicating a fault condition) and force the microgird system to operate in its islanded mode. However, in its autonomous mode the microgrid is more vulnerable since it will not be able to synchronize its frequency and voltage setpoints using grid values as references. Hence, attackers can compromise local controllers and sensors to create voltage and frequency instabilities. Additionally, adversaries can manipulate load sharing patterns among different power generation resources within the microgrid (e.g., inverters, storage systems, controllable loads, etc.) to disrupt optimal scheduling [3]. In Algorithm 1, we present the post-installation attack methodology followed by the rootkit.

The rootkit can remain passively inside the host system until the assignment of a malicious target objective. For example, if the rootkit aims to create frequency deviations, it will use the virtual twin of the microgrid to identify the optimal agents that can achieve this objective. It will then start manipulating power and frequency sensors which feed inputs to the DG-level inverter control. A coordinated attack targeting multiple DGs continues until the desired level of instability has been achieved. After the target objective is completed, the rootkit modifies the measurements before they are reported to system observers (to disguise its presence) and remains inactive until a new attack is instructed.

Algorithm 1 Proposed Rootkit Attack Methodology

1: Eavesdrop on compromised agents to collect real-time state information.
2: Use the acquired information to build a data-driven twin model of the system.
3: Determine the malicious objective (e.g., voltage instability, frequency instability, disturbances in load sharing schemes between multiple sources, etc.)
4: Identify a time frame to achieve the set objective and mark specific time slots at which manipulations will be introduced.
5: Initiate sensor perturbations while remaining hidden from security mechanisms.
6: Use the system's data-driven model to predict the future state information.
7: Send the *predicted* values to system observers masking its presence and attack impacts.
8: Use the designed data-driven model to identify the agents, which, if manipulated, can achieve the target objectives.
9: Alter voltage and current measurements at the PCC level to create artificial fault conditions and force defensive microgrid islanding.
10: During autonomous microgrid operation, modify the frequency and voltage reference values, and manipulate the setpoints of power devices.
11: Disguise the rootkit's actions to remain hidden from security mechanisms and carry out future attacks undetected.

3 CONCLUSION AND FUTURE WORK

Rootkits acquire and use system knowledge to mask their presence inside a target system and perform malicious actions without being detected. Rootkits in cyber-physical systems, like microgrids, can manipulate asset operations creating instability and cascading impacts. This paper discusses the operating strategy of a microgrid-based rootkit which can perform coordinated attacks targeting both devices at the local DGs and the PCC. The malware leverages a data-driven virtual twin of the system to mask its operation and attack impacts. The rootkit can also mislead security mechanisms and trigger erroneous islanding, which renders microgrids vulnerable to multiple attacks. Our future work of this concept will provide experimental and simulation results and design robust detection and mitigation mechanisms against such stealthy rootkit attacks, enhancing microgrid security and resiliency.

REFERENCES

[1] Prashanth Krishnamurthy, Hossein Salehghaffari, Shiva Duraisamy, Ramesh Karri, and Farshad Khorrami. 2019. Stealthy Rootkits in Smart Grid Controllers. In *2019 IEEE 37th International Conference on Computer Design (ICCD)*. 20–28.
[2] Abraham Peedikayil Kuruvila, Ioannis Zografopoulos, Kanad Basu, and Charalambos Konstantinou. 2021. Hardware-assisted detection of firmware attacks in inverter-based cyberphysical microgrids. *International Journal of Electrical Power & Energy Systems* 132 (2021), 107150.
[3] Juan Ospina, Xiaorui Liu, Charalambos Konstantinou, and Yury Dvorkin. 2021. On the Feasibility of Load-Changing Attacks in Power Systems During the COVID-19 Pandemic. *IEEE Access* 9 (2021), 2545–2563.
[4] Suman Rath, Diptak Pal, Parth Sarthi Sharma, and Bijaya Ketan Panigrahi. 2020. A cyber-secure distributed control architecture for autonomous AC microgrid. *IEEE Systems Journal (Early Access)* (2020).
[5] Ioannis Zografopoulos, Juan Ospina, Xiaorui Liu, and Charalambos Konstantinou. 2021. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. *IEEE Access* 9 (2021), 29775–29818.