Behind Closed Doors

Process-Level Rootkit Attacks in Cyber-Physical Microgrid Systems

Rath, Suman ; Zografopoulos, Ioannis ; Vergara , Pedro P.; Nikolaidis, Vassilis C. ; Konstantinou, Charalambos

DOI
10.1109/PESGM48719.2022.9916907

Publication date
2022

Document Version
Final published version

Published in
Proceedings of the 2022 IEEE Power & Energy Society General Meeting (PESGM)

Behind Closed Doors: Process-Level Rootkit Attacks in Cyber-Physical Microgrid Systems

Suman Rath[*], **Ioannis Zografopoulos**[†], **Pedro P. Vergara**[‡], **Vassilis C. Nikolaidis**[§], **Charalambos Konstantinou**[†]
[*]School of Electrical & Computer Engineering, Oklahoma State University
[†]CEMSE Division, King Abdullah University of Science and Technology (KAUST)
[‡]Intelligent Electrical Power Grids, Delft University of Technology (TU Delft)
[§]Dept. of Electrical and Computer Engineering, Democritus University of Thrace
E-mail: suman.rath@okstate.edu, p.p.vergarabarrios@tudelft.nl, vnikolai@ee.duth.gr
{ioannis.zografopoulos, charalambos.konstantinou}@kaust.edu.sa

2022 IEEE Power & Energy Society General Meeting (PESGM) | 978-1-6654-0823-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/PESGM48719.2022.9916907

***Abstract*—Embedded controllers, sensors, actuators, advanced metering infrastructure, etc. are cornerstone components of cyber-physical energy systems such as microgrids (MGs). Harnessing their monitoring and control functionalities, sophisticated schemes enhancing MG stability can be deployed. However, the deployment of 'smart' assets increases the threat surface. Power systems possess mechanisms capable of detecting abnormal operations. Furthermore, the lack of sophistication in attack strategies can render them detectable since they blindly violate power system semantics. On the other hand, the recent increase of process-aware rootkits that can attain persistence and compromise operations in undetectable ways requires special attention. In this work, we investigate the steps followed by stealthy rootkits at the process level of control systems pre- and post-compromise. We investigate the rootkits' precompromise stage involving the deployment to multiple system locations and aggregation of system-specific information to build a neural network-based virtual data-driven model (VDDM) of the system. Then, during the weaponization phase, we demonstrate how the VDDM measurement predictions are paramount, first to orchestrate crippling attacks from multiple system standpoints, maximizing the impact, and second, impede detection blinding system operator situational awareness.**

***Index Terms*—Rootkit, cyber-physical microgrid, intelligent malware, data-driven prediction, virtual twin.**

I. Introduction

Microgrids (MGs), among others, foster the inclusion of renewable energy sources. Closely coupled cyber and physical layers guarantee the increased flexibility and robust operation of MGs. The information and communication cyber layer receives inputs from sensors and issues controls in the physical layer. As a result, adversaries can exploit cyber vulnerabilities (e.g., insecure protocols, software bugs, etc.) to port their attacks impacting MG's control and stability [1]. Attacks able to manipulate sensor data can have significant impacts (e.g., blackouts, human safety, equipment damage, etc.) [2].

Existing literature focuses on various cyberattacks, their exploitation techniques, and schemes to detect and mitigate them [3]. The severity and risks associated with malware infections within industrial systems, especially rootkits, has captured the attention of researchers [4]. Rootkits represent a class of malware which can intelligently hide their presence inside their targets [5]. They can eavesdrop system data and allow attackers to collect real-time system information via remotely accessible connections [6]. Adversaries can exploit these connections to issue malicious commands, manipulate the infected device(s), and stealthily control their operation.

MG-based process level rootkit attacks should be considered when designing and implementing detection and mitigation strategies. Rootkit attacks should represent a crucial part of reliability assessment procedures for certification laboratories, tasked with identifying and eliminating vulnerabilities in embedded control devices and designing experimental testbeds for evaluation of cyber-physical power systems [4], [7]. This paper extends our previous work-in-progress on stealthy rootkit attacks [8], and highlights a potential rootkit attack path after the installation of the malware at multiple locations within the MG. After its deployment, the rootkit aggregates system measurements to build an accurate system replica allowing the estimation of the MG states trajectories; in our case, using a neural network-based approach. We demonstrate different approaches that rootkits could utilize to conceal their presence (during the system information aggregation phase) and disguise the attack impact overcoming existing security fortifications exploiting system state estimations. The paper presents simulation results to demonstrate the attack methodology and achievable system impact.

II. Attack Model

Rootkits can leverage the vulnerabilities (cyber layer) of operating system architectures encountered in power system workstations, HMIs, etc. during their deployment. Persistence is then achieved by masking their presence through system information and log modifications [9]. In most cases, the compromised systems exhibit vulnerabilities similar to consumer computers, and rootkits can exploit them to deploy on different levels of the hardware or software stack, e.g., firmware, bootloader, memory, kernel -based rootkits, etc. In Fig. 1, we present a MG model infected with the rootkit. Our threat model assumes that the rootkit can access and stealthily modify process level sensor measurements and controller strategies at different locations within the MG, i.e., a strong adversary model [3]. The rootkit achieves persistence and disguises its operation, by collecting sufficient system data to anticipate the MG state trajectories. By reporting the expected

978-1-6654-0823-3/22/$31.00 ©2022 IEEE

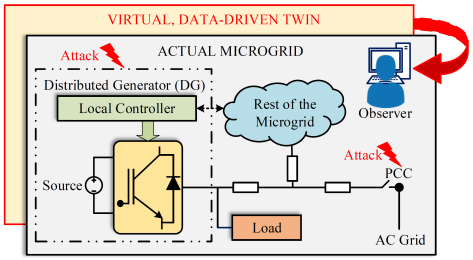

Fig. 1. Microgrid (MG) rootkit attack model.

values, the rootkit remains undetected by system operators, while maximizing its potential attack impact.

In this work, we build on the concept of process level rootkit attacks hiding their presence in cyber-physical MGs [8]. Once the rootkit gains access to various MG elements (e.g., controllers, actuators, etc.), it starts eavesdropping on the system information. Such process level data could include state parameters (e.g., voltage, frequency, etc.) utilized to build a virtual data-driven model (VDDM); similar to a digital twin of the entire MG. The granularity of the VDDM depends on the attacker's goal, capabilities, and available resources. The model is then employed to predict future system states and control operations. The attacker uses the predicted values of the VDDM MG to bypass security mechanisms and remain undetected. The attack aims to create gradual changes at the local distributed generation (DG) level whose effects can propagate through grid devices (e.g., controllers, inverters, etc.) impacting the overall power system.

The changes can range from minor alterations, like voltage injections with minor effects on system performance, to noise additions in sensor measurements which can generate erroneous control inputs to grid devices affecting the power generation, voltage stability, and introducing harmonic frequencies [10]. Although such perturbations might be small in magnitude to remain undetected, their impact can increase over prolonged periods of time and threaten nominal system operation [11].

The malware is able to intelligently coordinate the manipulation of power electronic converters at both the DG level and the point of common coupling (PCC) to maximize its impact. For example, 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 MG to operate in islanded/autonomous mode (i.e., by tripping its circuit breaker). However, in such operation mode the MG is more vulnerable since it will not be able to synchronize its frequency and voltage setpoints using grid values as references. Thus, adversaries can compromise local controllers and sensors to create voltage and frequency instabilities. Additionally, manipulation of load sharing patterns among different power generation resources within the MG can disrupt the optimal scheduling [12]. In Algorithm 1, we present the post-installation attack methodology followed by the rootkit.

The rootkit operates non-intrusively inside the host until the assignment of a malicious target objective. For instance, if the rootkit aims to create frequency deviations, it will use the MG's VDDM to identify the subset of agents that will achieve this objective. It will then manipulate power and frequency sensors providing inputs to the DG-level inverter control. The attack targeting multiple DGs, continues until the desired level of instability is achieved. After the target objective is completed, the rootkit modifies the measurements before being reported to system observers (to disguise its presence) and remains inactive until a new attack is performed.

Algorithm 1 Process level rootkit attack methodology.

1: Eavesdrop vulnerable devices to collect measurements.
2: Use acquired measurements to construct a VDDM of the system. Train ANN-based estimator for state prediction.
3: Identify malicious objective (e.g., frequency/voltage instability, disturbances in optimal load sharing, etc.).
4: Use the VDDM to identify the devices which can be manipulated to achieve the set objective.
5: Determine a time frame for the attack when the system is vulnerable and/or rootkit actions will not trigger alarms.
6: Modify sensor measurements at the PCC level to create artificial fault conditions, forcing defensive islanding.
7: During autonomous operation, alter the frequency and voltage references and the setpoints of power devices.
8: Modify sensor measurements and use the ANN-based state estimator to predict the nominal system state.
9: Mask rootkit manipulation by reporting the *predicted* values to the MG observer(s).

III. Control and Attack Formulation

The control framework of the MG has a hybrid structure with a central master controller at the PCC-level and one distributed local controller at each DG. This structure consists of primary, secondary, and tertiary control mechanisms. The primary controller is responsible for the load sharing among the DGs, and has a droop-based control objective which is achieved through frequency and voltage regulation as follows:

$$\omega_i^* = \omega_n - D_{P_i} P_i \tag{1}$$

$$v_i^* = v_n - D_{Q_i} Q_i \tag{2}$$

where ω_i^* and v_i^* represent frequency and voltage of i^{th} DG, ω_n and v_n denote nominal frequency and voltage, and P_i and Q_i the active and reactive power measurements of the i^{th} DG. D_{P_i} and D_{Q_i} are the droop coefficients determined considering the following (for a N-DG MG):

$$D_{P_1} P_1 = D_{P_2} P_2 = ... = D_{P_N} P_N = \Delta\omega_{Th} \tag{3}$$

$$D_{Q_1} Q_1 = D_{Q_2} Q_2 = ... = D_{Q_N} Q_N = \Delta v_{Th} \tag{4}$$

where $\Delta\omega_{Th}$ and Δv_{Th} represent the maximum permissible deviation of frequency and voltage, respectively.

In the grid-connected mode, the grid determines frequency and voltage values [13]. In this case, the load sharing pattern is regulated through the modification of ω_n and v_n. As demonstrated in Eqs. (1) and (2), the actions of the primary controller will cause a droop in the trajectory of frequency and voltage as the values of P and Q increase. To solve this issue and restore the system parameters to their nominal trajectories,

978-1-6654-0823-3/22/$31.00 ©2022 IEEE

the secondary controller introduces $\delta\omega$ and δv terms in the power controller equations:

$$\omega_i^* = \omega_n - D_{P_i} P_i + \delta\omega \tag{5}$$

$$v_i^* = v_n - D_{Q_i} Q_i + \delta v \tag{6}$$

In Eqs. (5) and (6), $\delta\omega$ and δv negate the droop caused as a result of the primary control. They are defined as follows [1]:

$$\begin{aligned}\delta\dot{\omega} = K_1\Big(\sum_{j\epsilon N(i)} a_{ij}(\omega_j - \omega_i) + g_i(\omega_n - \omega_i) \\ + \sum_{j\epsilon N(i)} a_{ij}(D_{P_j} P_j - D_{P_i} P_i)\Big)\end{aligned} \tag{7}$$

$$\delta\dot{v} = K_2\Big(\sum_{j\epsilon N(i)} a_{ij}(D_{Q_j} Q_j - D_{Q_i} Q_i)\Big) \tag{8}$$

where a_{ij} represents the element in the adjacency matrix of the bidirectional connected communication graph, g represents the pinning gain, and K_1, K_2 are constants [1]. The control targets for the secondary controller are shown below:

$$\lim_{t\to\infty} ||\omega_i(t) - \omega_n|| = 0 \; \forall \; i \tag{9}$$

$$\lim_{t\to\infty} ||D_{Pi} P_i - D_{Pj} P_j|| = 0 \; \forall \; i, \; j \tag{10}$$

$$\lim_{t\to\infty} ||D_{Qi} Q_i - D_{Qj} Q_j|| = 0 \; \forall \; i, \; j \tag{11}$$

The rootkit's long-term target is to disrupt the aforementioned control objectives by introducing small manipulationswhose consequences are unnoticeable by bad data detectors (BDDs). The rootkit methodology and the steps required for the attack are discussed in the following sections.

A. VDDM: Target Identification and State Prediction

In recent days, virtual power plants (VPPs) have been widely used for the modeling of demand-response management schemes, participation in day-ahead markets, etc. [14], [15]. Open source data enable adversaries to access and build such VPPs for malicious gains [16]. In our use case, the adversary uses the VDDM of the MG for two purposes: *(i)* performance evaluation of an attack vector before its introduction in the physical system, and *(ii)* prediction of system behaviour under normal conditions to hide the rootkit's manipulations from the system, e.g., BDDs.

Before initiating an attack, the adversary attempts to infect the maximum possible agents at the sensor, communication, and controller levels to maximize possible data collection. However, in a practical scenario, the attacker's ability to install malware at different stages may be limited by physical, hardware, or software constraints [17], [18]. In that case, the attacker can construct a virtual replica of the system with limited state information. Thus, the virtual system may not be a precise replica of the actual system and its accuracy will be determined by the quality of the data captured and the adversary's knowledge about the system [3]. The replica, in our work, uses a combination of Kalman filtering (KF) and neural networks to predict the future states of the MG. Specifically, KF is used to train an artificial neural network (ANN) that acts as the state estimator. It improves the quality and size of the training dataset by estimating missing values of data [19]. KF can also generate a sufficiently large dataset from a relatively smaller set of accurate data points, eliminating any potential uncertainty associated with the rootkit's data collection abilities (which may affect training of the VDDM). The hybrid estimator – combining KF and ANN – improves prediction accuracy and convergence speed when compared with traditional KF/NN approaches [20], [21]. The steps involved in the generation of the training and test datasets for the ANN are described below.

Since the attacker has access to sensors and controllers, real-time measurements from a set of infected physical sensors ζ can be captured. The state of the system is estimated from the captured measurements using KF Let the vector containing the measurements (obtained from ζ) be m. The system state is:

$$x(t) = F(t)x(t-1) + B(t)c(t) + n(t) \tag{12}$$

where $x(t)$, $F(t)$, $B(t)$, $c(t)$, $n(t)$ represent the state vector, the state transition matrix, the control input matrix, the control input vector, and the unknown process noise vector corresponding to $x(t)$, respectively. $n(t)$ is given by a zero mean normal distribution provided by the covariance matrix $C_0(t)$, $E[n(t)n(t)'] = C_0(t)$. The equation depicting the measurement can be written as follows.

$$m(t) = H(t)x(t) + v(t) \tag{13}$$

where $H(t)$ and $v(t)$ represent the transformation matrix mapping states to measurements and the known process noise vector, respectively. $v(t)$ is obtained from the covariance matrix $C_1(t)$, $E[v(t)v(t)'] = C_1(t)$. The state in the next time step can be estimated as follows:

$$x(t+1|t) = F(t)x(t|t) + B(t)c(t) \tag{14}$$

$$m(t+1|t) = H(t)x(t+1|t) \tag{15}$$

$$n(t+1) = m(t+1) - m(t+1|t) \tag{16}$$

Further,

$$x(t+1|t+1) = x(t+1|t) + N(t+1)n(t+1) \tag{17}$$

where $N(t+1)$ represents the Kalman gain utilized for state covariance. The state covariance can be estimated as:

$$P(t+1|t) = F(t)P(t|t)F(t)' + C_0(t) \tag{18}$$

$$S(t+1) = H(t+1)P(t+1|t)H(t+1)' + C_1(t+1) \tag{19}$$

$$N(t+1) = P(t+1)H(t+1)'S(t+1) - 1 \tag{20}$$

$$P(t+1|t+1) = P(t+1|t) - N(t+1)S(t+1)N(t+1)' \tag{21}$$

where $P(t+1|t)$, $S(t+1)$, $N(t+1)$ and $P(t+1|t+1)$ are the state prediction covariance, measurement covariance, filter gain, and updated state covariance, respectively.

The measurements collected by the rootkit, are used to analyze the current state and estimate the future states of the system. Furthermore, the obtained data is used to perform

978-1-6654-0823-3/22/$31.00 ©2022 IEEE

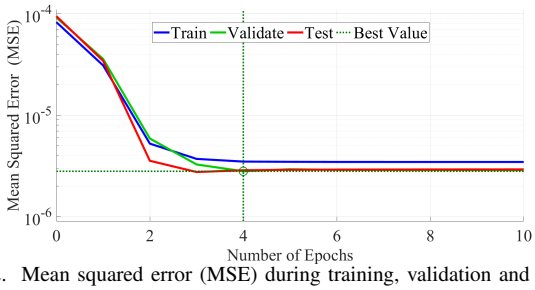

Fig. 2. Mean squared error (MSE) during training, validation and testing of the artificial neural network (ANN).

supervised training of an ANN with a l-layer feed-forward architecture that can predict the future state X_P of the system once it receives the measurement vector m and the requisite estimation time T as inputs. Let the initial set of weights (defined during the training phase) be W_0. The initial output X_{P0} can be defined as:

$$X_{P0} = f_A(W_0, l, m, T) \tag{22}$$

As the training progresses, the weights are updated through back-propagation (post-completion of each iteration) to minimize the error in the outputs per the predefined loss function.

$$W_{i+1} = f_B(\eta, e, W_i, l) \tag{23}$$

where η is the learning rate, and e represents the error between output of the network (after the i_{th} iteration) and the estimated output from the training data.

The predicted state (output) after the i_{th} iteration can be defined as a function mapping the obtained measurements (input) to the future state, given a set of weights W_i.

$$X_{Pi} = f_A(W_i, l, m, T) \tag{24}$$

After convergence, the network can be deployed for state estimation in the malicious system. Before the attack vector α introduction, the attacker tries to estimate the future system state X_{P_α, T_α} using the malicious VDDM.

$$X_{P_\alpha, T_\alpha} = f_A(W_f, l, m + \alpha, T_\alpha) \tag{25}$$

where T_α represents the end of the attack period. The magnitude of α must satisfy the following constraint: $|\alpha| \leq |\alpha_{max}|$, where $|\alpha_{max}|$ represents the maximum allowable magnitude of the attack vector to evade BDDs. During the weaponization phase, the attacker estimates and reports the expected normal system state to conceal the rootkit actions.

$$X_{N\alpha, T\alpha} = f_A(W_f, l, m, T_\alpha) \tag{26}$$

where $X_{N\alpha, T\alpha}$ is the predicted normal trajectory of the system in the absence of the attack vector α.

IV. Results and Discussion

An AC MG model is designed using MATLAB following the architecture of the model presented in [1]. The model consists of four DGs. Details of various system parameters can be obtained from [1]. Data collected from this test model is used to generate a VDDM, which can predict the future states of the system using the KF-ANN hybrid state estimator model discussed in Section III. The ANN is trained through

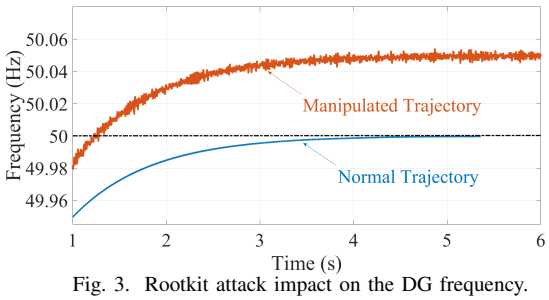

Fig. 3. Rootkit attack impact on the DG frequency.

supervised learning using labelled datasets generated from the designed MG model and the KF algorithm. Fig. 2 shows the accuracy of the VDDM by depicting the mean squared error (MSE) during the training, validation and testing phases.

The MG model is also used as a test system to demonstrate the possible impact that a rootkit malware with partial/complete access can cause to disrupt nominal behavior. Three target objectives are assigned to the malicious rootkit: *(i)* frequency manipulation, *(ii)* voltage manipulation, and *(iii)* disruption of load sharing. For these objectives, the rootkit uses its controller- and sensor-level access at the PCC side to first create a false fault alarm, cause defensive islanding of the system, and then compromise the DG operation.

A. Target: Frequency Manipulation

When the adversary instructs the rootkit to initiate the frequency manipulation attack, the malware evaluates its access level and uses the malicious VDDM to identify the vulnerable agents, which can be exploited to achieve the desired level of deviation. In this case, the adversarial objective entails achieving a higher steady state frequency. To accomplish this, the rootkit manipulates load devices and sensors. It modifies ω_n affecting $\delta\omega$ as per Eq. (7) and further influences ω_i^* as per Eq. (5). Fig. 3 depicts the normal and manipulated system trajectories after forced islanding. The rootkit can successfully distort the system frequency trajectory through the manipulation of load sensors and the local controller associated with the leader, i.e., DG 1. Fig. 3 shows that the frequency attains steady state at 50.05 Hz, however, the deviation could be further increased depending on the introduced attack vector.

B. Target: Voltage Manipulation

In the voltage manipulation case, the rootkit malware can either modify the voltage levels at any particular bus or create voltage instability affecting the whole MG system. After the target assignment, the malware uses the VDDM to determine the manipulation strategy required to achieve the set objective. In our case, the rootkit introduces false reactive power demand by thoroughly crafting bias injections to the system sensors. Fig. 4 and Fig. 5 show the normal voltage trajectory and the voltage trajectory after the rootkit manipulations are initiated. The experimental results demonstrate that the rootkit attack can cause the gradual increase of the three-phase voltage magnitude at DG 1.

978-1-6654-0823-3/22/$31.00 ©2022 IEEE

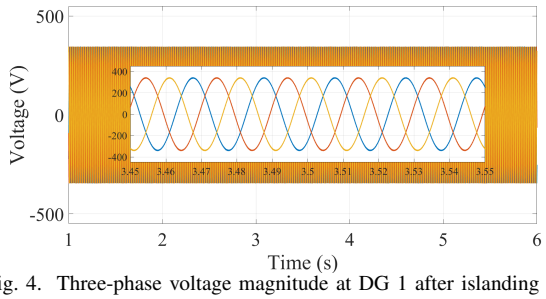

Fig. 4. Three-phase voltage magnitude at DG 1 after islanding occurs.

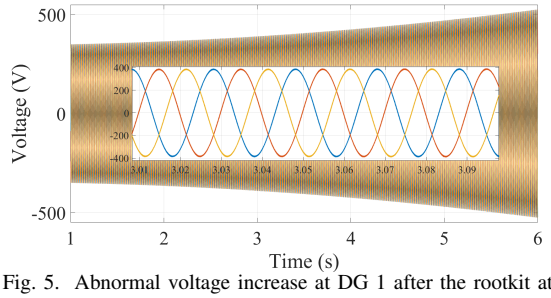

Fig. 5. Abnormal voltage increase at DG 1 after the rootkit attack.

C. Target: Disturbance in Load Sharing

In the attack-free scenario, all DGs in the simulated system share the total load demand equally (load sharing pattern shown in Fig. 6). However, during the attack phase, the rootkit disrupts the existing load sharing pattern. After the vulnerable agent identification, the malware establishes a time frame ($t = 5s$) within which manipulations will be introduced. For instance, an attack could be initiated during peak demand when the DGs operate close to their generation limits. Fig. 7 shows the disruption in load sharing caused by the rootkit through controller-level manipulation. Continued manipulations destabilize the system (after $t = 5s$) creating instabilities.

V. Conclusions and Future Work

The impact of process-aware rootkit attacks represents a severe threat for power systems. The presented rootkit can learn the MG's operational patterns. We demonstrate how such information can help mount crippling attacks against the local DGs and the PCC level. Rootkits can achieve persistence by masking their presence. Our future work will focus on developing detection and mitigation mechanisms, e.g., moving target defences, stable kernel represenations [22], etc. thwarting the adversarial learning behavior of rootkits.

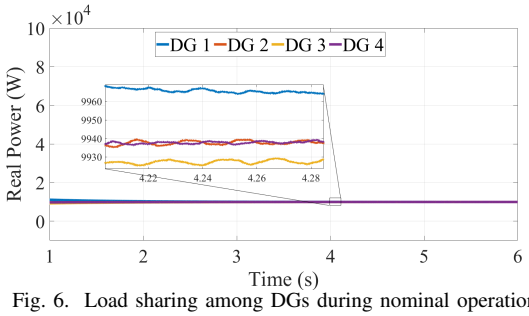

Fig. 6. Load sharing among DGs during nominal operation.

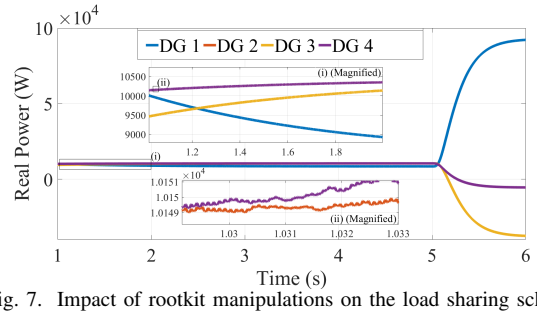

Fig. 7. Impact of rootkit manipulations on the load sharing scheme.

References

[1] S. Rath *et al.*, "A cyber-secure distributed control architecture for autonomous ac microgrid," *IEEE Systems Journal*, vol. 15, no. 3, 2021.

[2] C. Konstantinou *et al.*, "Gps spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment," *IET Cyber-Physical Systems: Theory & Applications*, vol. 2, no. 4, pp. 180–187, 2017.

[3] I. Zografopoulos *et al.*, "Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies," *IEEE Access*, vol. 9, pp. 29 775–29 818, 2021.

[4] J. Powers *et al.*, "Whitelist malware defense for embedded control system devices," in *Saudi Arabia Smart Grid (SASG)*. IEEE, 2015.

[5] P. Krishnamurthy *et al.*, "Stealthy rootkits in smart grid controllers," in *International Conference on Computer Design (ICCD)*, 2019, pp. 20–28.

[6] C. Xenofontos *et al.*, "Consumer, commercial and industrial iot(in) security: attack taxonomy and case studies," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 199–221, 2022.

[7] J. Reeves *et al.*, "Intrusion detection for resource-constrained embedded control systems in the power grid," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 2, pp. 74–83, 2012.

[8] S. Rath, I. Zografopoulos, and C. Konstantinou, "Stealthy rootkit attacks on cyber-physical microgrids: Poster," in *Proceedings of the 12th ACM Int'l Conference on Future Energy Systems*. ACM, 2021, p. 294–295.

[9] MITRE. Rootkit. [Online]. Available: https://tinyurl.com/2p83p89n

[10] A. P. Kuruvila *et al.*, "Hardware-assisted detection of firmware attacks in inverter-based cyberphysical microgrids," *International Journal of Electrical Power & Energy Systems*, vol. 132, p. 107150, 2021.

[11] M. Leng, S. Sahoo, and F. Blaabjerg, "Stability investigation of dc microgrids under stealth cyber attacks," in *2021 IEEE Energy Conversion Congress and Exposition (ECCE)*, 2021, pp. 1427–1432.

[12] J. Ospina *et al.*, "On the feasibility of load-changing attacks in power systems during the covid-19 pandemic," *IEEE Access*, vol. 9, 2021.

[13] A. Bidram *et al.*, *Cooperative synchronization in distributed microgrid control*. Springer, 2017.

[14] A. Mnatsakanyan and S. W. Kennedy, "A novel demand response model with an application for a virtual power plant," *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 230–237, 2014.

[15] A. Baringo, L. Baringo, and J. M. Arroyo, "Day-ahead self-scheduling of a virtual power plant in energy and reserve electricity markets under uncertainty," *IEEE Transactions on Power Systems*, vol. 34, no. 3, 2018.

[16] A. Keliris *et al.*, "Open source intelligence for energy sector cyberattacks," in *Critical infrastructure security and resilience*. Springer, 2019.

[17] X. Wang *et al.*, "Malicious firmware detection with hardware performance counters," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 2, no. 3, pp. 160–173, 2016.

[18] O. M. Anubi and C. Konstantinou, "Enhanced resilient state estimation using data-driven auxiliary models," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 639–647, 2019.

[19] R. Habtom and L. Litz, "Estimation of unmeasured inputs using recurrent neural networks and the extended kalman filter," in *Proceedings of International Conference on Neural Networks*, vol. 4. IEEE, 1997.

[20] P. M. Sieberg *et al.*, "Hybrid state estimation-a contribution towards reliability enhancement of artificial neural network estimators," *IEEE Transactions on Intelligent Transportation Systems*, 2021.

[21] R. Zhan and J. Wan, "Neural network-aided adaptive unscented kalman filter for nonlinear state estimation," *IEEE Signal Processing Letters*, vol. 13, no. 7, pp. 445–448, 2006.

[22] I. Zografopoulos and C. Konstantinou, "Detection of malicious attacks in autonomous cyber-physical inverter-based microgrids," *IEEE Transactions on Industrial Informatics*, 2021.

978-1-6654-0823-3/22/$31.00 ©2022 IEEE