21, rue d'Artois, F-75008 PARIS
http://www.cigre.org

PS2-11

D2 Colloquium 2019

Cyber Attack and Defense for Smart Inverters in a Distribution System

C. -C. SUN[1], R. ZHU[2], C. -C. LIU[1,2]

[1]Washington State University, [2]Virginia Polytechnic Institute and State University

USA

SUMMARY

The fast-growing installation of solar PVs has a significant impact on the operation of distribution systems. Grid-tied solar inverters provide reactive power capability to support the voltage profile in a distribution system. In comparison with traditional inverters, smart inverters have the capability of real-time remote control through digital communication interfaces. However, cyberattack has become a major threat with the deployment of Information and Communications Technology (ICT) in a smart grid. The past cyberattack incidents have demonstrated how attackers can sabotage a power grid through digital communication systems. In the worst case, numerous electricity consumers can experience a major and extended power outage. Unfortunately, tracking techniques are not efficient for today's advanced communication networks. Therefore, a reliable cyber protection system is a necessary defense tool for the power grid.

In this paper, a signature-based Intrusion Detection System (IDS) is developed to detect cyber intrusions of a distribution system with a high level penetration of solar energy. To identify cyberattack events, an attack table is constructed based on the Temporal Failure Propagation Graph (TFPG) technique. It includes the information of potential cyberattack patterns in terms of attack types and time sequence of anomaly events. Once the detected anomaly events are matched with any of the predefined attack patterns, it is judged to be a cyberattack. Since the attack patterns are distinguishable from other system failures, it reduces the false positive rate. To study the impact of cyberattacks on solar devices and validate the performance of the proposed IDS, a realistic Cyber-Physical System (CPS) simulation environment available at Virginia Tech (VT) is used to develop an interconnection between the cyber and power system models. The CPS model demonstrates how communication system anomalies can impact the physical system. The results of two example cyberattack test cases are obtained with the IEEE 13 node test feeder system and the power system simulator, DIgSILENT PowerFactory.

KEYWORDS

Cyber attacks – Distributed energy resources – Cyber security – Smart inverter – Intrusion detection system

ccliu@vt.edu

1 INTRODUCTION

Electric power grids are being transformed into smart grids by extensive deployment of ICTs in both transmission and distribution systems. Remote control and data acquisition as well as automation functions improve the efficiency of power system operations. However, cyber-physical security against cyber intrusions have become a major concern as more ICTs are integrated into the grid. In recent years, Distributed Energy Resource (DER) devices have been installed as energy resources in a smart grid. At the third quarter of 2018, the installed solar energy has reached 60 GW in the U.S. [1]. To be connected through the SCADA network, traditional inverters have been upgraded to smart inverters with a two-way communication interface. This upgrade also creates potential cyber vulnerabilities to intruders. In addition, a high penetration level of PV generation has brought new challenges in system reliability [2]. The voltage regulation mechanisms [3], [4] are deployed to maintain the voltage level within an acceptable range. However, attackers might target these control technologies to cause a collapse of a distribution system. Moreover, False Data Injection (FDI) attacks have threatened smart grid applications [5]. In 2015, the cyberattack on the Ukrainian power grid demonstrated that cyber intrusions can caused a major power outage on a power system [6]. In a NESCOR report [7], failure scenarios caused by cyberattacks on Distributed Energy Resource (DER) communication networks have been reported, indicating that DER devices are vulnerable to cyber intrusions. Although cyber security of a smart grid has been studied [8-11], research on the attack and defense for smart inverters is a new topic that represents a growing concern of industry and government.

Cyber security for a distribution system with DER generation and control devices has been assessed by using a three-stage Defender-Attacker-Defender (DAD) game theory [12]. The proposed assessment method provides a guideline for finding the weaknesses and establishing effective defense strategies. In [13], cyber security challenges due to the integration of DER devices have been introduced. The authors also propose a holistic attack resilient framework to protect the DER infrastructure against cyberattack events. As an energy source in a smart grid, critical DER devices may be compromised and impact the reliability of a distribution system. An attack-mitigation model has been proposed in [14]. The interactions between attackers and utilities are formulated as a nonlinear differential game. Reference [15] provides a detection algorithm against voltage control attacks in a distribution system with PV systems. Although a falsified voltage measurement injection attack does not impact PV systems directly, the violation of feeder voltage regulation can activate the control scheme (e.g., Volt-Var control) which is embedded in smart inverters.

This paper proposes an on-line detection system to identify suspicious abnormal behaviors that deviate from the regular operations of a smart inverter. Based on the real-time voltage reading on a feeder, smart inverters should follow the operation code to enable the assigned control mode. For different reactive power output conditions (i.e., absorbing and injecting), a smart inverter has a corresponding pattern for power factor readings. The IDS utilizes cause-effect relations of abnormal behaviors defined in the proposed attack table. It uses chronological relations among anomaly events to list the possible attack paths in a smart inverter. By comparing the similarity between detected anomalies and each possible attack path in the attack table, the proposed IDS is able to determine the likelihood of a cyber attack.

The remainder of this paper is organized as follows. Section 2 describes an architecture of DER networks, including communication and physical devices. Section 3 presents the detection algorithm for smart inverters. In Section 4, a hardware-in-the-loop testbed for this research is introduced. Section 5 provides the test results of the proposed intrusion detection system for smart inverters. The conclusion is stated in Section 6.

2 COMMUNCIATION ARCHITECTURE OF DER NETWORK

As far as cyber security is concerned, the most critical devices in a DER network are smart inverters. Grid-tied renewable energy resources, such as wind turbines and PV panels, need an electrical inverter to convert DC into AC power and then send it to a power grid. Smart inverters are monitored and controlled via a communication system from a control center. To regulate interconnected DER devices, the IEC Technical Committee 57, Working Group (WG) 17 has released IEC 61850-90-7 providing

specific object models for power converters in DER systems, while IEC 61850-7-420 provides abstract information models for general data exchanges. The Smart Inverter Working Group (SIWG) has updated Rule 21 to California Public Utilities Commission (CPUC) in 2014, providing a three-phase approach to regulate DER systems [16]. IEEE 2030.5, also known as Smart Energy Profile 2.0 (SEP 2), is suggested to be the default protocol which should be supported by three types of individual DER communication devices, including: (1) Generating Facility Energy Management Systems (GFEMS), (2) data aggregators, and (3) SMart inverter Control Unit (SMCU). According to the latest implementation guide for smart inverters [17], the IEEE 2030.5 protocol implements "A client/server model based on a REpresentational State Transfer (REST) architecture utilizing the core HTTP methods of GET, HEAD, PUT, POST, and DELETE." Figure 1 shows the two communication configurations between a utility and remote devices in a DER system that are included in Rule 21.

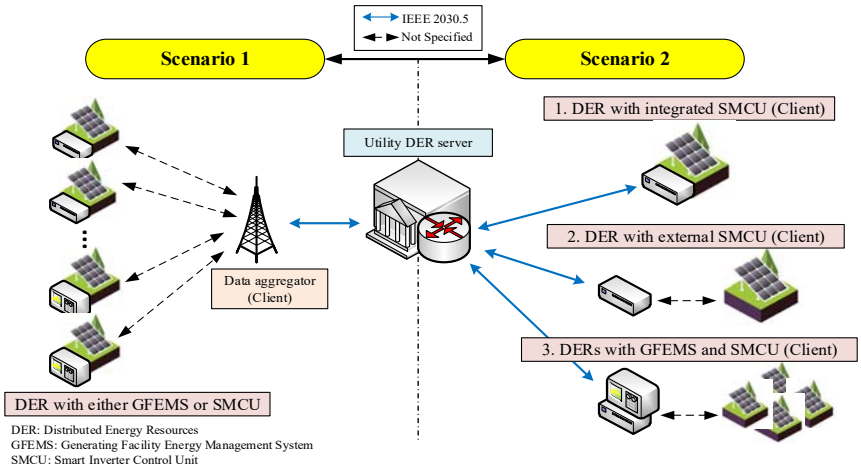


Figure 1: Communication structure of a DER system in compliance with IEEE 2030.5 standard

3 DETECTION SYSTEM AND ALOGORITHM

3.1 Attack Table

A proposed attack table is developed for defining anomaly paths of each threat type. TFPG is one of the model-based diagnosis techniques for a dynamic system [18]. It is used to capture the causal and temporal relationships between failures and consequences in a system. This feature can be used for modeling temporal relationships between anomaly events (causes) and attack types (effects). Figure 2 shows an example of TFPG models for cyberattacks in a DER system. Node a, b, c, d and g are the anomaly events in the cyber domain, whereas nodes e, f, h and i are in physical devices. Most of the anomaly types (i.e., node a to g) can be acquired by system and security logs, events and behaviors of smart inverters. Node "*h*" indicates that a smart inverter is switched to an inappropriate control mode under the corresponding voltage level in a power grid. Table I specifies the default control modes of smart inverters and the corresponding trends of power measurement readings (smart inverters, not power grid) during different voltage events. Any violation is considered and reported as an anomaly to IDS. For example, in an over voltage event, smart inverters should switch to Volt-Var control mode to mitigate the voltage problem. According to the power output diagram in Figure 3, a smart inverter has two options to react to the over voltage event:

(1) Absorbing more reactive power from a grid if a smart inverter operates in Area I: Since more reactive power (inductive) is consumed and active power setting does not change, the PF value should drop.

(2) Reducing the reactive power output if a smart inverter operates in Area II: Since less reactive output (capacitive) is produced and active power setting does not change, the PF value should increase.

The normal behaviors for under voltage event can be obtained by the same concept above. When the grid voltage level is measured within $\pm 5\%$ range from rated value (i.e., 1 p.u.) [19], smart inverters should run under Maximum Power Point Tracking (MPPT) to maximize the active power output. The PF and power flow trends are based on the I-V curve of a PV system. At node "*i*," the measurement readings are compared among a smart inverter and grid sensors (e.g., smart meter, micro PMU, etc.). For example, it is regarded as an anomaly if a voltage reading is different between a smart inverter and SCADA system.

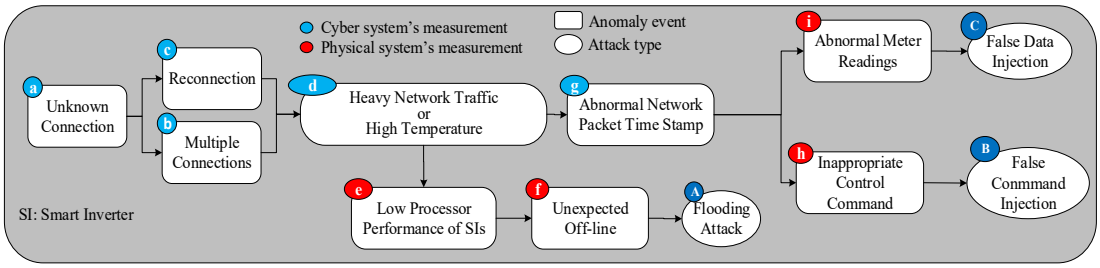


Figure 2: Intrusion processes of a DER system based on TFPG model

Table I: Operation table for smart inverter control modes

Voltage Event	Control Mode	Operation Area (Figure 3)	Power Factor Trend	Reactive Power Flow Trend ($\|Var\|$)
Over Voltage	Volt-Var	I	Decrease	Increase
		II	Increase	Decrease
Under Voltage	Volt-Var	I	Increase	Decrease
		II	Decrease	Increase
Normal	MPPT	I and II	Refer to MPPT	

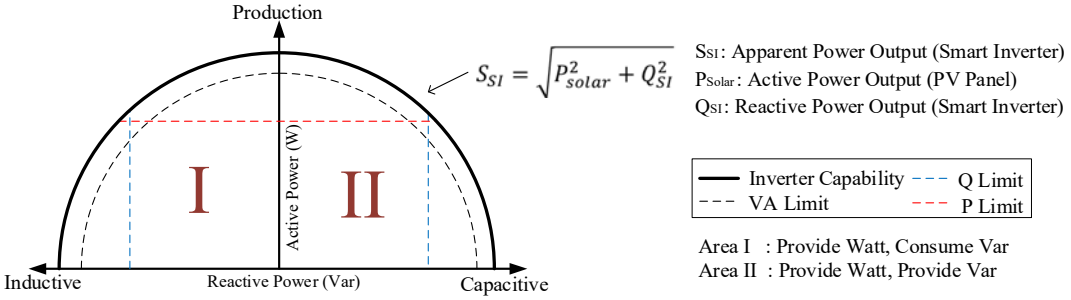


Figure 3: Working area for smart inverters

3.2 Patern Recognition Algorithm

To design an IDS, two assumptions are made: (1) intruders' actions are assumed to follow the sequence in the proposed attack paths in Figure 2, and (2) The detection system is assumed to have false alarms (both false positive and negative) occasionally. With the assumptions, the detection problem can be transformed into a problem of spelling correction of English words. In the attack model, each anomaly event is assigned with an English letter as shown in Figure 2. Each path, $P = \{P_{1a}, P_{1b}, P_{2a}, P_{2b}, P_{3a}, P_{3b}\}$, from the first node (i.e., node a) to an attack type node (i.e., node A, B and C) is regraded as an English phrase in a dictionary which is listed in Table II. Once the first anomaly event has been detected, the IDS will start to record the sequence of anomaly events as an input to

Spelling Correction System (SCS) [20], [21]. At each time stamp, SCS calculates the minimum edit distance, ED_{min}, between the input string and each phrase in the dictionary. Edit distance, d_{ij}, is defined as the minimum number of edit operations that transform first i characters of one string into first j chracters of another string. The edit operations are defined as: (1) insert a single letter, (2) delete a single letter, and (3) substitute a single letter by any letter that is not identical with the original one. According to Wagner-Fischer algorithm [22], each operation counts as a unit cost. The matching process is formulated as Eqation (3.1) to (3.4), where "a" is a detected string and "b" is a string in the dictionary. Strings a and b consist of the number of m and n letters, respectively. Each of $W_{del}, W_{ins}\ and\ W_{sub}$ denotes the unit cost of the defined edit operations.

$$d_{i0} = \sum_{k=1}^{i} W_{del}(b_k) \qquad for\ 1 \le i \le m \tag{3.1}$$

$$d_{0j} = \sum_{k=1}^{j} W_{ins}(a_k) \qquad for\ 1 \le j \le n \tag{3.2}$$

$$d_{ij} = \begin{cases} d_{i-1,j-1} & for\ \ a_j = b_i \\ min\begin{cases} d_{i-1,j} + w_{del}(b_i) \\ d_{i,j-1} + w_{ins}(a_j) \\ d_{i-1,j-1} + w_{sub}(a_j, b_i) \end{cases} \end{cases} \tag{3.3}$$

$$ED_{min} = d_{mn} \tag{3.4}$$

Then, an attack similarity index, ATS_{ind}, is defined as:

$$ATS_{ind} = 1 - \frac{ED_{min}}{Length(detected\ string)} \tag{3.5}$$

Once ATS_{ind} is greater than a user-define threshold value V_{th}, the detected event is regarded as an intrusion event.

Table II: Attack route set generating from attack table.

Path	Attack Type	Dictionary
P_{1a}	Flooding attack	a→b→d→e→f
P_{1b}		a→c→d→e→f
P_{2a}	False command injection attack	a→b→d→g→h
P_{2b}		a→c→d→g→h
P_{3a}	False data injection	a→b→d→g→i
P_{3b}		a→c→d→g→i

4 CYBER-PHYSICAL SECURITY SIMULATION ENVIRONMENT

Figure 4 shows the structure of the proposed CPS simulation environment at Virginia Tech. The selected power system simulator has the model of a physical distribution system. In addition, it has an embedded OPC communication client that interconnects the cyber system model via the OPC server. Since Queuing theory is used to describe time delays [23] in a communication system, a Queue based cyber system model is developed by using MATLAB Simulink to simulate a DER communication network. A 3-Level structure for DER communication system is presented in Figure 4. In Level 1, distribution control center installs multiple applications that are needed to determine what commands and requests should be sent to which DER system. A Distribution Management System (DMS) helps operators control/monitor a distribution system by collecting grid data through a digital communication system. Once the distribution system is under a special operating condition, operators issue control commands to the field devices (e.g., smart inverters and circuit breakers). These signals will be transmitted to Level

2. In Level 2, GFEMS passes the signals to corresponding DER systems, while SMCUs are connected to physical DER systems (e.g. photovoltaic systems, wind farms) in Level 3.

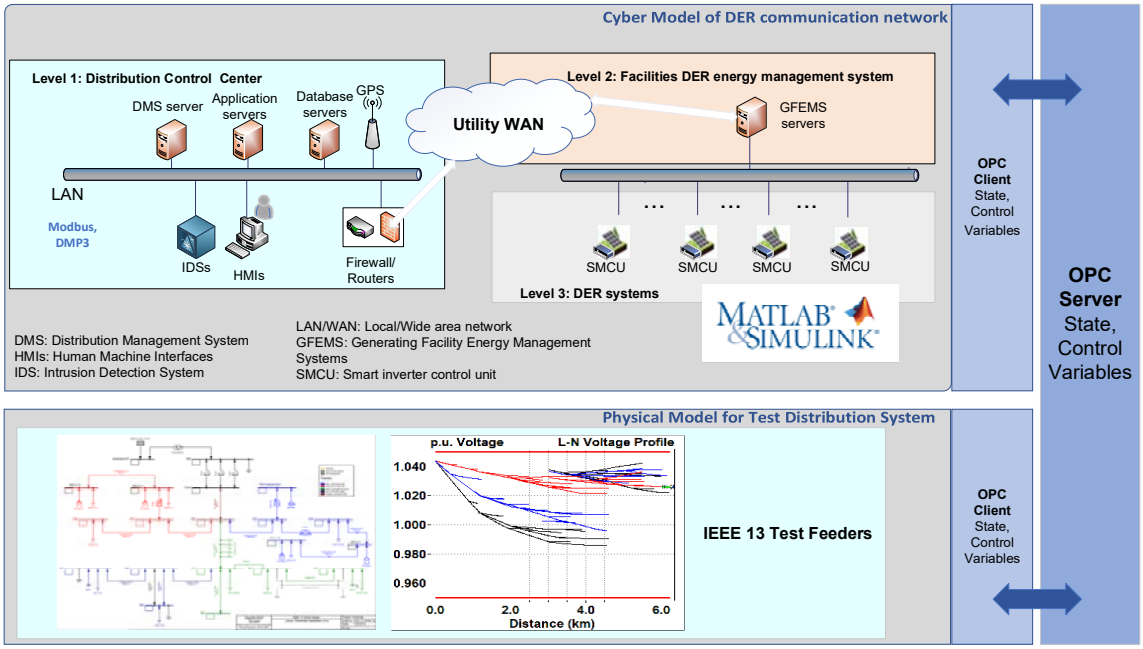


Figure 4: VT cyber-physical security simulation environment for DER system

5 CASE STUDY

Two cyber intrusion scenarios, flooding attack and false command injection attack, are tested using the proposed CPS simulation environment. The IEEE 13 Nodes Feeders Distribution System is used for illustration of the proposed cyber intrusions. As shown in Figure 5, six PV systems with different irradiance are connected to the feeders. Note that three PV systems, connected to single phase feeder 611, 645 LV1, and 645 LV2, respectively, are single phase PV systems with 40 kVA capacity. The other 3 PV systems are three phase PV systems with a 125 kVA capacity. Also, based on the settings from IEEE standard 1547-2018, the initial power factor of all PV systems is set to 1.

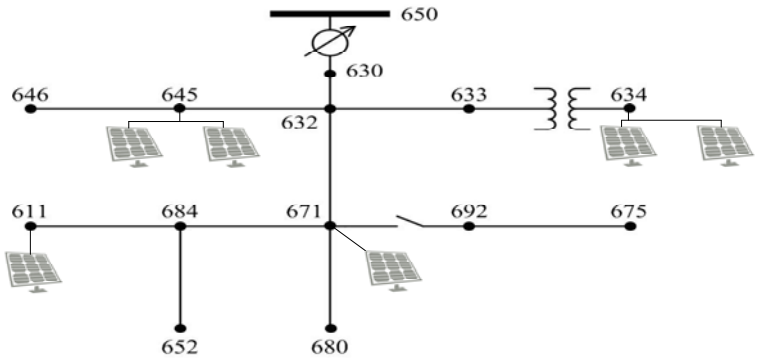


Figure 5: IEEE 13 Nodes Feeders with PV systems

5.1 Flooding Attack

The attack steps in the first test scenario are listed as follows: (1) Attackers establish a connection to a smart inverter, (2) To explore the weakness of a smart inverter, attackers log in to the targeted smart inverter multiple times, (3) Attackers launch a flooding attack by sending dummy packets, and (4) The

heavy network traffic causes low processor performance of a smarter inverter, ultimately leading to inaccessibility. Under this attack, the connection between the distribution control center and SMCU is blocked. Therefore, once the synchronized machine connected to feeder 633 is tripped, the under voltage event take places. As shown in Figure 6, the blue curve represents the voltage profile under a flooding attack. Since all control commands for Volt-Var control are blocked, the voltage magnitudes decreased sharply to approximately 0.9 p.u. at each feeder, except for Feeder 650 which is directly connected to substation. The flooding attack caused the PV system to be disabled so that it is no longer able to provide reactive power support in an under voltage event.

The aforementioned attack was tracked by the security logs. As shown in Table III, the proposed IDS accessed the logs from both cyber system and physical system and derived the anomaly events sequence as "a→b→c→d→e→f." Using the pattern recognition process from Equation (3.1) to (3.4) in terms of the detected sequence and each attack path in Table II, the detected sequence in both attack paths P_{1a} and P_{1b} provide the same minimum edit distance ED_{min} as 1. In Equation (3.5), the corresponding attack similarity index ATS_{ind} is 0.833 which is greater than the user-defined threshold V_{th}, 0.7. Thus, the IDS recognizes this scenario as a flooding attack. Once the attack is detected, as shown in Figure 6, the red curve indicates the voltage profile when PV systems are successfully switched to Volt-Var control modes. The comparison of the simulation results presents that Volt-Var control of smart inverters is enabled for voltage control.

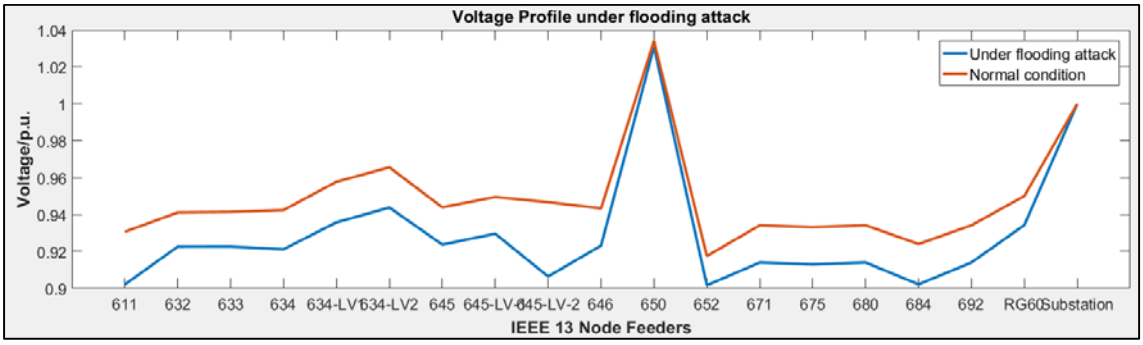
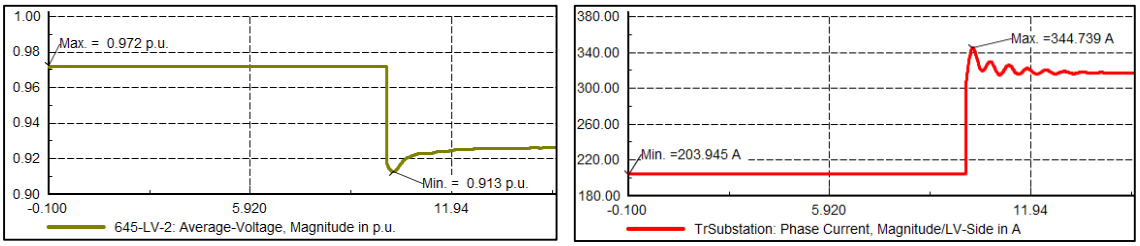


Figure 6: Comparison of voltage profiles under a flooding attack

5.2 False Command Injection Attack

In the second scenario, attackers injected the false commands to GFEMS servers, which pass the malicious commands to the smart inverters in the system. The abnormal connection process from the attackers is identical with first scenario. Besides that, the abnormal time stamps of network packets are recorded in security logs. Also, logs of the physical system indicates impropriate control commands for switching off the smart inverters. As shown in Table III, the proposed IDS detected the anomaly events sequence as "a→b→c→d→g→h." By using the same detection steps, the attack similarity index ATS_{ind} is found to be 0.833 which is greater than the V_{th}. Since the high ATS_{ind} value is given by attack paths P_{2a} and P_{2b}, the IDS recognizes this scenario as a false command injection attack. Since the attackers injected a switching signal through the DER communication system, the smart inverters are disconnected from the distribution system. As a result, Figure 7(a) shows the variation of voltages at Feeder 645 exceeds the 5% operating limit. In Figure 7(b), the current magnitude of the distribution substation increases sharply after the disconnection of smart inverters. The simulation results indicate that the test distribution system loses reactive power capability. In addition, the distribution substation has to provide more power to meet the reactive power demand. An overloaded condition can trigger the transformer protection in the substation due to overcurrent. By NEC 450.3 standard [24], fuses or circuit breakers are designed to react to the overcurrent condition at the source substation. Once the breaker is opened, the cyber attack causes a power outage in the test system.



(a) **(b)**

Figure 7: Distribution system response for false command injection attack: (a) voltage magnitude at feeder 634, and (b) current magnitude at source substation

Table III: Results of detection system for cyberattack scenarios

Detection System	**Anomaly Events Sequence** (Cyber and Physical systems measurements)	**Pattern Recognition Algorithm**			
		Attack route sets from Dictionary	Edit Manipulations of Anomaly Event Sequence	ED_{min}	ATS_{ind}
Scenario 1	a→b→c→d→e→f	P_{1a}: a→b→d→e→f	• Delete "c"	1 (min)	0.833
		P_{1b}: a→c→d→e→f	• Delete "b"	1 (min)	
		P_{2a}: a→b→d→g→h	• Delete "c" • Substitute "e" by "g" • Substitute "f" by "h"	3	
		P_{2b}: a→c→d→g→h	• Delete "b" • Substitute "e" by "g" • Substitute "f" by "h"	3	
		P_{3a}: a→b→d→g→i	• Delete "c" • Substitute "e" by "g" • Substitute "f" by "i"	3	
		P_{3c}: a→c→d→g→i	• Delete "b" • Substitute "e" by "g" • Substitute "f" by "i"	3	
Scenario 2	a→b→c→d→g→h	P_{2a}: a→b→d→g→h	• Delete "c"	1 (min)	0.833
		P_{2b}: a→c→d→g→h	• Delete "b"	1 (min)	

6 CONCLUSION

Since the number of distributed renewable generation is growing drastically in terms of generation capacity and number of devices, cyber attacks have become a major threat to the reliable and secure operation of a distribution system. This paper proposes an on-line IDS to protect DER networks against potential cyber intrusions. The proposed detection mechanism is able to identify three attack types by matching the attack sequences between the proposed attack table and detected events. A realistic CPS simulation environment is developed to study the impact of cyber attacks and validate the cyber defense sytem. Two cyber attack cases are evaluated to demonstrate how cyber attacks can impact a power system. The proposed IDS is validated with well known cyber attack scenarios. The test results show that the detection algorithm is able to identify the cyber attacks in a smart inverter.

ACKNOWLEDGEMENT

This research is supported by U.S. National Science Foundation under the award number ECCS-1824577 at Virginia Tech, a Collaborative Project with Ohio State University. We also thank U.S. Department of Energy for their funding under project Grid Modernization Laboratory Consortium (GMLC) Project GM0100

BIBLIOGRAPHY

[1] Solar Energy Industries Association. "Solar State by State," Washington D.C., USA, SEIA, 2018. [Online]. Available at: https://www.seia.org/states-map.

[2] R. Seguin, J. Woyak, D. Costyk, J. Hambrick, and B. Mather. "High-Penetration PV Integration Handbook for Distribution Engineers," Denver CO, USA, National Renewable Energy Laboratory (NREL), January 2016. [Online]. Available at: https://www.nrel.gov/docs/fy16osti/63114.pdf.

[3] L. Wang, F. Bai, R. Yan, and T. K. Saha. "Real-Time Coordinated Voltage Control of PV Inverters and Energy Storage for Weak Networks with High PV Penetration," IEEE Transactions on Power Systems, vol. 33, No. 3, March 2018, pp. 3383–3395. DOI: 10.1109/TPWRS.2018.2789897

[4] N. Mahmud, A. Zahedi, and A. Mahmud. "A Cooperative Operation of Novel PV Inverter Control Scheme and Storage Energy Management System Based on ANFIS for Voltage Regulation of grid-Tied PV System," IEEE Transactions on Industrial Informatics, vol. 13, No. 5, January 2017, pp. 2657–2668. DOI: 10.1109/TII.2017.2651111

[5] P.-Y. Chen, S. Yang, J. A. McCann, J. Lin, and X. Yang. "Detection of False Data Injection Attacks in Smart-Grid Systems," IEEE Communications Magazine, vol. 53, No. 2, February 2015, pp. 206–213. DOI: 10.1109/MCOM.2015.7045410.

[6] M. J. Assante, T. Conway, and R. M. Lee. "TLP: White Analysis of the Cyber Attack on the Ukrainian Power Grid," Washington D.C., USA, E-ISAC, 2016. [Online]. Available at: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[7] National Electric Sector Cybersecurity Organization Resource. "Electric Sector Failure Scenarios and Impact Analyses" Palo Alto CA, USA, Electric Power Research Institute (EPRI), 2013.

[8] C.-C. Sun, C.-C. Liu, and J. Xie. "Cyber-Physical System Security of a Power Grid: State-of-the-Art," Electronics, vol. 5, No. 4, July 2016, p. 40. DOI: 10.3390/electronics5030040.

[9] C.-C. Sun, A. Hahn, and C.-C. Liu. "Cyber Security of a Power Grid: State-of-the-Art," International Journal of Electrical Power & Energy Systems, vol. 99, July 2018, pp. 45–56. DOI: 10.1016/j.ijepes.2017.12.020.

[10] J. Hong, C.-C. Liu, and M. Govindarasu "Integrated Anomaly Detection for Cyber Security of the Substations," IEEE Transactions on Smart Grid, vol. 5, No. 4, July 2014, pp. 1643–1653. DOI: 10.1109/TSG.2013.2294473.

[11] H. He and J. Yan. "Cyber-Physical Attacks and Defences in the Smart Grid: A Survey," IET Cyber-Physical Systems: Theory & Applications, vol. 1, No. 1, December 2016, pp. 13–27. DOI: 10.1049/iet-cps.2016.0019.

[12] D. Shelar and S. Amin. "Security Assessment of Electricity Distribution Networks Under DER Node Compromises," IEEE Transactions on Control of Network Systems, vol. 4, 2017, No. 1, March 2017, pp. 23-36. DOI: 10.1109/TCNS.2016.2598427

[13] J. Qi, A. Hahn, X. Lu, J. Wang, and C.-C. Liu. "Cybersecurity for Distributed Energy Resources and Smart Inverters," IET Cyber-Physical Systems: Theory & Applications vol. 1, No.1, December 2016, pp. 28-39.DOI: 10.1049/iet-cps.2016.0018.

[14] P. Srikantha and D. Kundur. "A DER Attack-Mitigation Differential Game for Smart Grid Security Analysis," IEEE Transactions on Smart Grid, vol. 7, No. 3, May 2016, pp. 1476–1485. DOI: 10.1109/TSG.2015.2466611.

[15] Y. Isozaki et al., "Detection of Cyber Attacks Against Voltage Control in Distribution Power Grids with PVs" IEEE Transactions on Smart Grid, vol. 7, No. 4, July 2016, pp. 1824–1835. DOI: 10.1109/TSG.2015.2427380.

[16] California Energy Commission and California Public Utilities Commission. "Recommendations for Utility Communications with Distributed Energy Resources (DER) Systems with Smart Inverters," Sacramento CA, USA, SIWG Phase 2, 2015. [Online]. Available at: https://www.energy.ca.gov/electricity_analysis/rule21/documents/SIWG_Phase_2_Communications_Recommendations_for_CPUC.pdf.

[17] Common Smart Inverter Profile Working Group. "IEEE 2030.5 Implementation Guide for Smart Inverters" San Jose CA, USA, SunSpec, March 2018. [Online]. Available at: https://sunspec.org/wp-content/uploads/2018/03/CSIPImplementationGuidev2.003-02-2018-1.pdf.

[18] S. Abdelwahed, G. Karsai, N. Mahadevan, and S. C. Ofsthun. "Practical Implementation of Diagnosis Systems using Timed Failure Propagation Graph Models," IEEE Transactions on Instrumentation and Measurement, vol. 58, No. 2, February 2009, pp. 240-247. DOI: 10.1109/TIM.2008.2005958.

[19] American National Standard for Electric Power Systems and Equipment - Voltage Ratings (60Hz). ANSI Standard C84.1-2016.

[20] T. Okuda, E. Tanaka, and T. Kasai. "A Method for the Correction of Garbled Words Based on the Levenshtein Metric," IEEE Transactions on Computers, vol. C-25, No. 2, February 1976. DOI: 10.1109/TC.1976.5009232.

[21] R. K. Chaurasiya, N. D. Londhe, and S. Ghosh. "A Novel Weighted Edit Distance-Based Spelling Correction Approach for Improving the Reliability of Devanagari Script-Based P300 Speller System," IEEE Access, vol. 4, October 2016, pp. 8184–8198. DOI: 10.1109/ACCESS.2016.2614494.

[22] W. Masek and M.A. Paterson. "A Faster Algorithm Computing String Edit Distances" Journal of Computer and System Sciences, vol. 20, No.1, February 1980, pp. 18-31. DOI: 10.1016/0022-0000(80)90002-1.

[23] A. Stefanov and C.-C. Liu. "ICT Modeling for Integrated Simulation of Cyber-Physical Power Systems," 2012 3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe), Berlin, 2012, pp. 1-8. DOI: 10.1109/ISGTEurope.2012.6465730.

[24] National Fire Protection Agency (NFPA) NFPA70 Standard for Electrical Safety. "National Electrical Code," Quincy MA, USA, NFPA, 2017.