Stealthy False Data Injection Cyberattack Targeting Under Load Tap Changing Transformers in Smart Power Grid Causing Abnormal Voltage Profile

Ehsan Naderi
Department of Electrical Engineering, College of Engineering and Computer Science
Arkansas State University
Jonesboro, AR, USA
enaderi@astate.edu

Arash Asrari
Department of Electrical and Computer Engineering
Purdue University Northwest
Hammond, IN, USA
aasrari@pnw.edu

2024 Third International Conference on Power, Control and Computing Technologies (ICPC2T) | 979-8-3503-4920-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICPC2T60072.2024.10474991

***Abstract*—In the process of protecting power systems against different types of cyberattacks, the primary step is to precisely model such frameworks from attacker's perspective. This paper investigates a false data injection (FDI) attack framework, which can target under-load tap changing (ULTC) transformers, resulting in manipulated voltage profile in radial smart distribution networks. The developed FDI model compromises the voltage profile of a distribution feeder through misleading the volt/var optimization, that optimally manages system-wide voltage profile and flow of reactive power. The presented attack model is formulated as a bi-objective optimization problem. The objective functions from the attacker' s point of view are 1) minimizing the level of false data to be injected into the smart meters associated with load data and 2) maximizing the voltage deviation of the distribution grid. Negative impacts of such a cyberattack model have been validated and discussed in this work on an IEEE distribution test system, necessitating proper remedial actions, which will be elaborated in the next step of this research.**

Keywords—False data injection (FDI) attack, Pareto-optimal solution, smart distribution system, under load tap changer (ULTC), voltage imbalance

I. Introduction

A. Background, definitions, and Motivation

Tap changing transformer, which is the backbone of AC power grids, is widely used to minimize the voltage imbalance and maintain the voltage profile in the normal range of magnitude [1]. In active distribution systems, due to a large quantity of distributed generation (DG) units and their bidirectional power flow, voltage regulation is a critical issue, which can be addressed through vol-var optimization. However, automation and digitalization have transformed power networks into a new generation of power grids, called cyber-physical power systems (CPPS), where energy and information and communication technology (ICT) infrastructures meet [2]. Because of dependency on advanced metering equipment, CPPSs are highly vulnerable to different kinds of cyberattacks, among which false data injection (FDI) attacks dominate since they are easier to be performed by adversaries with little knowledge about the power grid [3]. The supervisory control and data acquisition (SCADA) network, for instance, makes it possible for attackers to falsify the recorded information and cause a variety of operational issues including congestion in transmission lines [4] and distribution branches [5], voltage violation [6], market power in deregulated electricity markets [7], etc. The following sub-section provides a detailed literature review on state-of-the-art research works scrutinizing FDI attacks targeting voltage control in smart power systems.

This research was supported in part by the National Science Foundation under Grant No. 2348420.

B. Related Works

Chen *et al*. proposed a reinforcement learning framework, oriented toward partial observable Markov decision process, for FDI cyberattacks to distort the normal operation of a power grid regulated by automatic voltage controls [8]. Chakrabarty and Sikdar developed a mechanism against stealthy FDI attacks targeting tap change commands through SCADA network affecting the normal voltage profile of the power system [9]. Ahmadzadeh *et al*. scrutinized an FDI framework based on which an adversary compromised voltage measurements in an active distribution grid leading to unacceptable voltage profile as well as the operation of protective components [10]. The authors in [10] also introduced a data driven detection technique to identify the affected voltage measurement and recognize the cyberattack. Choeum and Choi proposed a bi-level stealthy FDI attack on volt-var optimization function in distribution systems encompassing PV modules and capacitor banks. The consequence of such attacks was abnormal voltage profile along the medium voltage distribution feeder [11]. An FDI framework against voltage profile of smart distribution systems along with the corresponding appropriate false data detection mechanism were presented by Aysheh *et al*. in [12], where the impact of extensive PV plants on the voltage violations (i.e., both undervoltage and over voltage) was also scrutinized. Farroq *et al*. analyzed the negative impact of FDI attacks on the voltage quality control, controlled by the level of reactive power generation for PV modules, over a real distribution system in Northen Denmark [13]. Impact analysis of FDI cyberattacks targeting voltage stability (e.g., bus voltage magnitude and bus voltage phase angle) of power networks through calculation of

steady state voltage stability limit was introduced by Agrawal *et al.* in [14], where an attack constant was also defined to control the level of voltage imbalance from the attacker's standpoint. Finally, Rahimpour *et al*. presented a comprehensive review on the cybersecurity challenges of power transformers from different standpoints including attack type and consequence, prevention measures, detection mechanisms, etc. [15].

C. Research Gaps and Contribution of This Paper

In spite of the fact that extensive research efforts have been accomplished on investigating voltage profile abnormalities as a consequence of FDI cyberattacks targeting automatic voltage control in active distribution networks (e.g., [8]-[15]), the following research gaps is yet to be addressed in the existing literature.

- How to 1) model a bi-objective FDI framework to stealthy target under load tap changing (ULTC) transformers through compromising the results of volt-var optimization, 2) cause intended alteration to the tap position of the ULTC leading to extreme imbalance in the voltage profile, and 3) control the severity of the FDI attack from the attacker's point of view via achieving the non-dominated optimal solutions and saving them into a repository?

To the best of authors' knowledge, [11] is the only research work that proposed an FDI framework taking into account the volt-var optimization function to optimally inject false load data into the measurements resulting in deviation of voltage profile from the normal conditions. However, [11] did not take into account power loss and control actions associated with ULTC transformers, which can be seriously impacted by this type of cyberattack. To fill the indicated knowledge gap and address the aforementioned research questions, this paper develops a bi-objective optimization problem with two objective functions: 1) minimizing the amount of false information to be injected into the smart meters through solving a volt-var optimization problem by the operator in the substation and at the same time 2) maximizing the rate of deviation in the voltage profile of the smart distribution system from the reference voltage, which is equal to 1.00 p.u. Hence, a set of suboptimal solutions, referred to as non-dominated solutions or Pareto-optimal frontier, will be identified, which will verify the severity of this cyberattack for ULTCs within distribution systems.

II. Proposed Framework

Fig. 1 illustrates the proposed framework in this paper. According to this figure, one can perceive that an attacker launches an FDI cyberattack to inject false data into the smart meters through the advanced metering infrastructure (AMI). Then, the malicious information (shown by red dashed arrows in Fig. 1) will be fed to the volt-var optimization function, which is a part of the distribution management system. As a result, the volt-var optimization is performed via false data, consequently resulting in malicious calculating the optimal solutions (e.g., the position of tap associated with the ULTC transformer). The outcome of such an FDI attack will be abnormal voltage profile of the distribution systems through incorrect tap positions, obtained from the affected volt-var optimization problem in the distribution management system. This also leads to the degraded

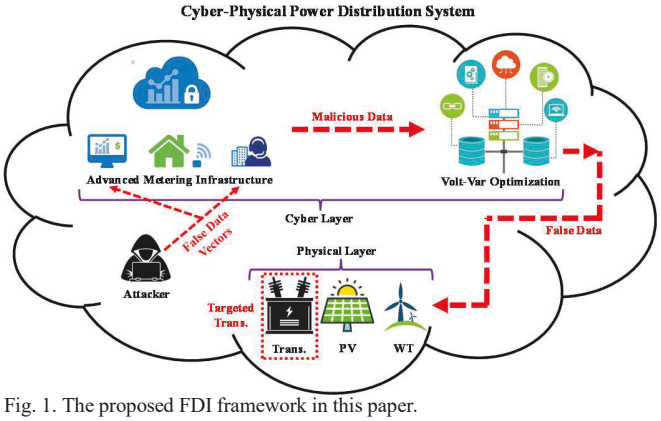

Fig. 1. The proposed FDI framework in this paper.

voltage profile and power quality for end-use customers. Validation of the proposed FDI framework and its negative impact on the distribution systems will be scrutinized in Section IV.B.

III. Problem Formulation

A. Multi-Objective Volt-Var Optimization

Three different objective functions are considered in the volt-var optimization problem, including 1) voltage deviation of buses, 2) active power losses, and 3) number of control actions for ULTC transformer. It is noted that the presented model takes into account a scheduling time period of τ for each objective function, which is to be minimized, as provided in (1)-(3).

$$OF_1 = \sum_{\tau=1}^{T}\sum_{b=1}^{B}|1.00 - V_b^{\tau}| \tag{1}$$

$$OF_2 = \sum_{\tau=1}^{T}\sum_{l=1}^{L} G_l \times \left(V_\tau^2 + \acute{V}_\tau^2 - 2 \times V_\tau^2 \times \acute{V}_\tau^2 \times \cos\left(\delta^\tau - \acute{\delta}^\tau\right)\right) \tag{2}$$

$$OF_3 = \sum_{\tau=1}^{T}\sum_{a=1}^{A} s_a^{\tau} \tag{3}$$

where B, T, L, and A are, respectively, the total number of buses, time intervals, lines, and control actions for ULTC; G_l is the conductance of line l; V and V' are the voltage amplitudes of buses at both side of line l; δ and δ' are the voltage phase angles associated with buses at both ends of like l; and s_a is the status of control equipment a.

The aggregated version of the objective functions (1)-(3) via penalty factors is minimized subject to sets of constraints including power equilibrium, operational restrictions, and limitations over the control variables. The complete list of the constraints in the volt-var optimization problem is presented in (4)-(10), where P_{PV}^{τ} (Q_{PV}^{τ}), P_{WT}^{τ} (Q_{WT}^{τ}), P_l^{τ} (Q_l^{τ}), and P_D^{τ} (Q_D^{τ}), are, respectively, the total active (reactive) power of PV modules, wind turbines, lines, and demands at time τ; G^{τ} and B^{τ} are conductance and susceptance of lines at time τ; V_{SS}^{τ} is the voltage of sub-station at time τ; Tap_{ULTC}^{τ} is the tap position of the ULTC at time τ; α_{ULTC} denotes the tap size for each tap alteration; P_d^{τ} and Q_d^{τ} are, respectively, the net active and reactive power associated with bus b at interval τ, which are the

summation of active/reactive power demand at bus b and active/reactive power related to renewable energy sources (i.e., PV modules and wind turbines) if bus b encompasses any renewable units; and V_{min} and V_{max} are the minimum and maximum acceptable voltage amplitudes.

$$P_{PV}^{\tau} + P_{WT}^{\tau} + P_{l}^{\tau} - P_{D}^{\tau} = V_{\tau} \sum_{B} \acute{V}_{\tau}(G^{\tau} \cos\delta^{\tau} + B^{\tau} \sin\delta^{\tau}) \quad (4)$$

$$Q_{PV}^{\tau} + Q_{WT}^{\tau} + Q_{l}^{\tau} - Q_{D}^{\tau} = V_{\tau} \sum_{B} \acute{V}_{\tau}(G^{\tau} \sin\delta^{\tau} - B^{\tau} \cos\delta^{\tau}) \quad (5)$$

$$V_{SS}^{\tau} = 1.00 + \alpha_{ULTC} \times Tap_{ULTC}^{\tau} \quad (6)$$

$$P_{load,b}^{\tau} - P_{PV,b}^{\tau} - P_{WT,b}^{\tau} = P_{d}^{\tau} \quad (7)$$

$$Q_{load,b}^{\tau} - Q_{PV,b}^{\tau} - Q_{WT,b}^{\tau} = Q_{d}^{\tau} \quad (8)$$

$$\sum_{\tau=1}^{T} \left| Tap_{ULTC}^{\tau} - Tap_{ULTC}^{\tau-1} \right| \leq A \quad (9)$$

$$V_{min} \leq V_{b}^{\tau} \leq V_{max} \quad (10)$$

Interested readers are directed to [16] for further details about the optimization problem and its constraints.

B. FDI Cyberattack Targeting ULTC

According to Fig. 1, the recorded measurements from smart meters are fed into the procedure of volt-var optimization via the advanced metering infrastructure, which is an integrated system of meters and data entities, enabling two-way communication between assets in modern power grids. However, an attacker injects false load data to the meters, resulting in stealthy alteration of the tap position of the ULTC. The consequence of such an FDI attack will be intended alteration in the magnitude of voltage along with the distribution feeder. In other words, increasing or decreasing the tap position, the attacker will be able to intentionally enhance and reduce the voltage profile, respectively. According to [11], if the voltage profile of the distribution grid is higher than the normal range, the efficiency of the distribution system will be negatively affected since the consequence of higher voltage profile is directly proportional to the power loss. Likewise, by decreasing the voltage profile below the acceptable range, the voltage stability of the system will be jeopardized, which will result in voltage collapse in extreme cases. The (to be minimized) objective function of the FDI cyberattack and its relevant constraints are presented as follows. It is noted that in the objective function (11), positive sign refers to the situation based on which the tap position of the ULTC transformer moves upward, consequently enhancing the voltage magnitude. Likewise, the negative sign highlights the situation based on which the tap position of the ULTC transformer switches downward, reducing the voltage magnitude of the corresponding bus (i.e., the targeted bus), consequently affecting the voltage profile of the entire distribution system.

$$OF_{1}^{Attack} = \Psi \sum_{b=1}^{B} \epsilon_{b}^{\tau} \pm Tap_{ULTC}^{\tau} \quad (11)$$

$$\sum_{b=1}^{B} \epsilon_{b}^{\tau} \leq N_{max}^{FSM} \quad (12)$$

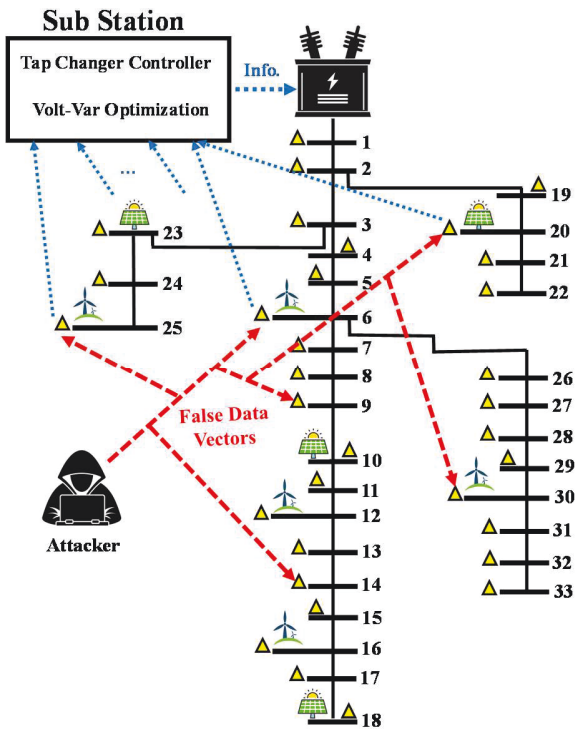

Fig. 2. Part of a typical smart distribution system under the developed FDI cyberattack and its different phases, according to Fig. 1.

$$\sum_{b=1}^{B} \Delta P_{b}^{\tau} = 0 = \sum_{b=1}^{B} \Delta Q_{b}^{\tau} \quad (13)$$

In (11)-(13), Ψ indicates the weight factor representing the attacker's effort, meaning that the higher the weight factor, the smaller the magnitude of the (to be injected) false data; ϵ_{b}^{τ} is the attack binary variable for bus b, meaning that if $\epsilon_{b}^{\tau} = 1$, bus b is targeted by the FDI attack; and N_{max}^{FM} is the maximum number of falsified meters.

After obtaining the falsified tap positions via solving (11)-(13), the attacker needs to feed the results obtained into the volt-var optimization problem (see Fig. 1) in order to push the ULTC transformer toward the wrong working point. Toward this end, Constraints (4)-(10) need to be updated to formulate the volt-var optimization problem from the attacker's point of view. The updated version of the integral constraints are provided in (14)-(15), where $\Delta P_{load,b}^{\tau}$ and $\Delta Q_{load,b}^{\tau}$ are, respectively, the injected malicious active and reactive load information associated with bus b at time interval τ; $\acute{P}_{PV,b}^{\tau}$ ($\acute{Q}_{PV,b}^{\tau}$) and $\acute{P}_{WT,b}^{\tau}$ ($\acute{Q}_{WT,b}^{\tau}$), denote the active (reactive) power corresponding to the PV modules and wind turbine, respectively, which are maliciously compromised during the FDI attack.

$$\begin{Bmatrix} (P_{load,b}^{\tau} \pm \Delta P_{load,b}^{\tau}) \\ -(P_{PV,b}^{\tau} \pm \acute{P}_{PV,b}^{\tau}) \\ -(P_{WT,b}^{\tau} \pm \acute{P}_{WT,b}^{\tau}) \end{Bmatrix} = P_{d,Attack}^{\tau} \quad (14)$$

$$\begin{Bmatrix} (Q_{load,b}^{\tau} \pm \Delta Q_{load,b}^{\tau}) \\ -(Q_{PV,b}^{\tau} \pm \acute{Q}_{PV,b}^{\tau}) \\ -(Q_{WT,b}^{\tau} \pm \acute{Q}_{WT,b}^{\tau}) \end{Bmatrix} = Q_{d,Attack}^{\tau} \quad (15)$$

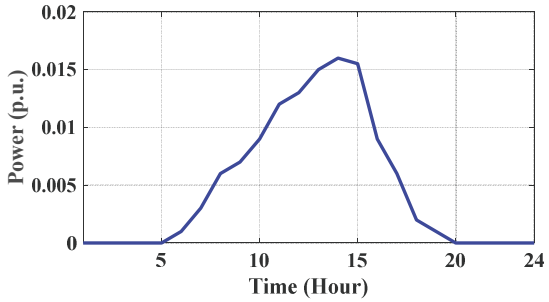

Fig. 3. The predicted active power profile for PV modules within the IEEE 33-bus test system.

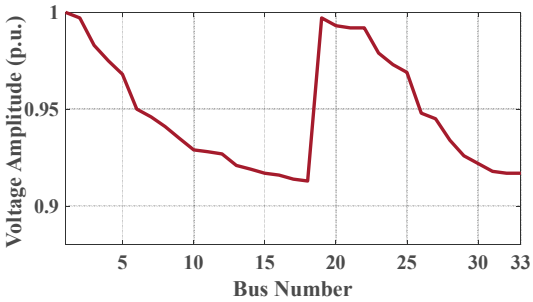

Fig. 4. The normal voltage profile of the IEEE 33 bus test system.

To obtain a deeper view about the proposed FDI cyberattack in this paper, Fig. 2 depicts the process on IEEE 33-bus smart distribution system, which is also the case study in this paper. It is noted that the yellow triangles, illustrated in Fig. 2, are smart meters associated with load data. In addition, the blue dotted arrows in Fig. 2 show the flow of information from smart meters to the control center running the volt-var optimization problem. The blue dotted arrows may or may not include malicious data.

The second objective function of the FDI attack, which is presented in (16), is to keep the false data vectors small enough to significantly reduce the chance of getting caught by the distribution system operator. Hence, attacker minimizes (16) to recognize the minimum false data vectors considering the operational constraints of the distribution grid (i.e., (4)-(10)).

$$OF_2^{Attack} = \sqrt{\sum_{b=1}^{B} \left(\Delta P_{load,b}^{\tau}\right)^2} \tag{16}$$

IV. Simulation Results and Analysis

A. Initialization

The developed attack framework was coded in MATLAB R2020b, and the simulations were performed in an Intel Core i7-13700 machine with 2.10 GHz clock frequency and 32 GB of RAM. Moreover, the power flow calculations were handled through MATPOWER 6.0 package, which is a capable tool assisting power system engineers handle the power flow studies [17]. The negative impacts of the developed FDI attack are evaluated on the modified IEEE 33-bus test distribution network in such a way that up to 35% of the overall demand can be supplied by solar panels and wind turbines (see Fig. 2). The distribution system includes one ULTC, 4 PV modules, 5 wind turbines, and 33 smart meters (i.e., one per bus), as shown by the yellow triangles in Fig. 2. The total active and reactive power demands on the system are, respectively, 3,715 kW and 2,300 kVAR. The rated power and diameter of wind turbines manufactured by Wind World [18] are, respectively, 250 kW and 29.2 m. Interested readers are directed to [19] for detailed information about PV modules and wind turbines distributed throughout the IEEE 33-bus test system. The predicted active power profile for PV plants is depicted in Fig. 3, and the normal voltage profile of the system is illustrated in Fig. 4. It is noted that the range of integer tap positions associated with the ULTC installed at the substation (see Fig. 2) is [-20, 20] with the step of 0.005. It is also noted that the maximum number of actions (i.e., tap alterations or A) is set to 5 during the scheduling time period, as presented by Constraint (9). The rest of the system data can be found in [19].

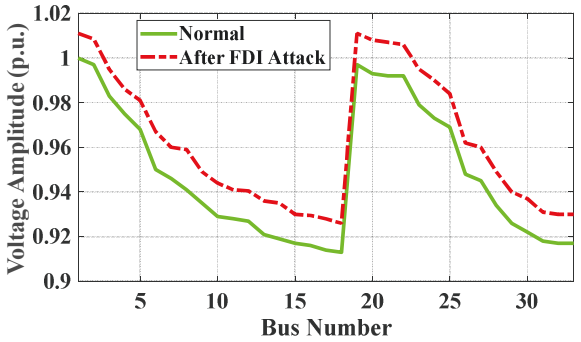

Fig. 5. The affected voltage profile of the IEEE 33-bus test system after launching the FDI cyberattack leading to overvoltage.

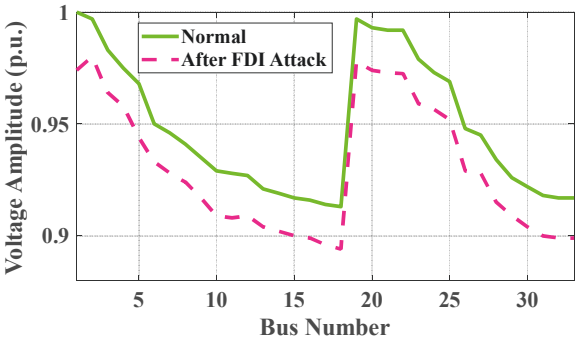

Fig. 6. The affected voltage profile of the IEEE 33-bus test system after launching the FDI cyberattack leading to undervoltage.

B. Obtained Results and Analyses

Fig. 5 presents the voltage profile of the distribution system at the time of the FDI attack leading to overvoltage, obtained after minimizing the objective function (11) with the positive sign. From this figure, one can infer that the distribution system is pushed toward higher voltage, consequently increasing the power loss of the system and disrupting the balance between active power and reactive power throughout the system.

To evaluate the other way around of the developed FDI attack (i.e., (11)-(13)), Fig. 6 depicts the voltage profile of the IEEE 33-bus test system after launching the attack resulting in undervoltage via taking into account the negative sign of the objective function (11). According to Figs. 5-6, it can be perceived that (11) can provide attacker with a mechanism to intentionally push the voltage profile of the IEEE 33-bus system

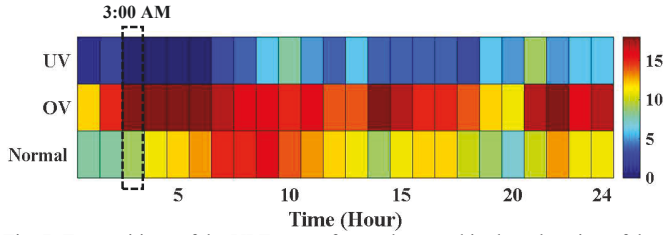

Fig. 7. Tap positions of the ULTC transformer loatcated in the substation of the IEEE 33-bus distribution system before and after the FDI cyberattacks compromising the voltahge profile. (OV: Overvoltage and UV: Undervoltage)

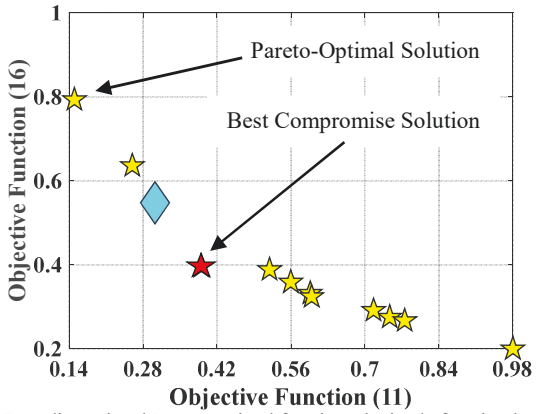

Fig. 8. Two-dimensional Pareto-optimal frontiers obtained after simultaneously minimizing (11) and (16), causing overvoltage.

toward his/her desired profiles. To obtain a better perspective about the contributing role of the ULTC in the affected voltage profiles of the IEEE 33-bus test system after the FDI cyberattacks (see Figs. 5-6), the tap positions of the ULTC transformer during the day are illustrated in Fig. 7. From this figure, it can be gathered that the FDI attacks managed to mislead the ULTC transformer located at the substation. For instance, the tap position of the ULTC is 8 at 3:00 AM (see the green block shown in Fig. 7), while the tap at the same time is moved to 18 (see the dark red block illustarted in Fig. 7) and 0 (see the dark blue block displayed in Fig. 7), respectively, pushing the voltage profile of the distribution grid toward higher and lower voltages.

Objective functions (11) and (16) were normalized via trapezoidal membership functions to bring their values to the range of [0, 1]. Fig. 8 shows the Pareto-optimal frontier associated with the presented FDI attack in (11)-(16). It is noted that the red pentagram illustrates the best compromise solution (BCS) between objective functions (11) and (16) when the importance degrees of these two objectives are 50%. From Fig. 8, one can perceive that the bi-objective approach for the FDI attack can provide attackers with a set of optimal solutions to control the severity of the cyberattack. For example, the affected voltage profiles of the IEEE 33-bus test system associated with the red pentagram is provided in Fig. 5. In addition, the malicious tap positions, corresponding to the FDI attack, that were depicted in Fig. 7 are related to the red pentagram of Fig. 8. If attacker selects another optimal solution form the repository, for instance the cyan diamond as displayed in Fig. 8, the number of tap alterations decreases since more false data are injected into the smart meters, consequenctly the severity of the FDI cyberattack reduces. The voltage profile of the IEEE 33-bus system after launching the developed FDI attack associeted with

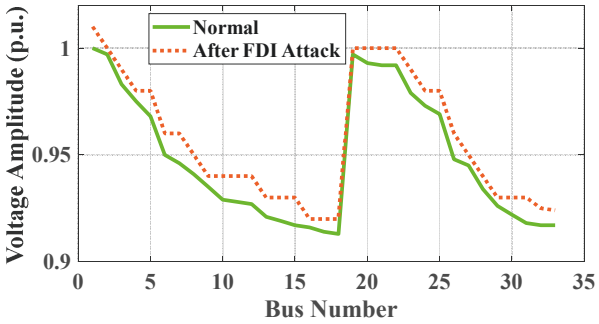

Fig. 9. Affected voltage profile of the IEEE 33-bus distribution system assoctaed with the cyan diamond at 5:00 AM (see Fig. 8).

the cyan diamond is presented in Fig. 9. It is noted that the importance degrees of the objective functions (11) and (16) are, respectively, 35% and 65% in the FDI attack associated with the cyan diamond (see Fig. 9). From Figs. 8-9, it can be concluded that multi-objective FDI attack frameworks can significantly jeoparadize the stability of power distibution networks; hence, remediating such cyberattacks need state-of-the-art remedial action schemes to alleviate the impacts of the attack and bring back the targeted system to the normal operation. This will be the scope of our future work.

V. Conclusion

A bi-objective false data injection (FDI) attack model was presented in this work, which can cause alterations in the normal voltage profile of smart distribution systems via manipulating the tap ratio of under load tap changing transformers (ULTCs). The objective functions were integrated to minimize the load data to be injected into the smart meters and minimize the number of changes applied to the tap position of the ULTC transformer. Data manipulation was accomplished through falsifying the results of volt-var optimization problem, consequently affecting the voltage profile of the distribution system toward higher or lower profiles compared to normalcy. The simulation results on the IEEE 33-bus distribution network confirmed that if attackers are equipped with such a mechanism, they can intentionally push the distribution system toward operational issues. This will definitely necessitate a proper remedial action scheme from the system operator's point of view, which will be elaborated in the next step of this research.

References

[1] I. Kim, "A method of modeling tap-changing transformers for power-flow and short-circuit analysis studies," *TENCON 2018 - IEEE Region 10 Conference*, Jeju, South Korea, 2018, pp. 0772-0775.

[2] D. Willenberg, P. Erlinghagen, and A. Schnettler, "Analysis of the impact of cyber attacks in active distribution grids onto the transient system stability," *IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, Sarajevo, Bosnia and Herzegovina, 2018, pp. 1-6.

[3] M. Jafari, M.A. Rahman, and S. Paudyal, "Optimal false data injection attacks against power system frequency stability," *IEEE Trans. Smart Grid*, vol. 14, no. 2, pp. 1276-1288, Mar. 2023.

[4] J. Khazaei, "Detection of cyber-physical attacks aiming at multi transmission line congestions using dynamic state-estimation," *IEEE Power & Energy Society General Meeting (PESGM)*, Washington, DC, USA, 2021, pp. 1-5.

[5] E. Naderi and A. Asrari, "Integrated power and transportation systems targeted by false data injection cyberattacks in a smart distribution

network," in *Electric Transportation Systems in Smart Power Grids - Integration, Aggregation, Ancillary Services, and Best Practices*, CRC Taylor & Francis Publisher, Boca Raton, FL, USA, 2023.

[6] Y. Isozaki *et al*., "On detection of cyber attacks against voltage control in distribution power grids," *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Venice, Italy, 2014, pp. 842-847.

[7] E. Naderi and A. Asrari, "A remedial action scheme to mitigate market power caused by cyberattacks targeting a smart distribution system," *IEEE Trans. Ind. Inform.*, Early Access, 2023, doi: 10.1109/TII.2023.3304049.

[8] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, "Evaluation of reinforcement learning-based false data injection attack to automatic voltage control," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2158-2169, Mar. 2019.

[9] S. Chakrabarty and B. Sikdar, "Detection of hidden transformer tap change command attacks in transmission networks," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5161-5173, Nov. 2020.

[10] M. Ahmadzadeh, A. Abazari, and M. Ghafouri, "Detection of FDI attacks on voltage regulation of PV-integrated distribution grids using machine learning methods," *IEEE Electrical Power and Energy Conference (EPEC)*, Victoria, BC, Canada, 2022, pp. 73-78.

[11] D. Choeum and D. -H. Choi, "OLTC-induced false data injection attack on volt/var optimization in distribution systems," *IEEE Access*, vol. 7, pp. 34508-34520, 2019.

[12] N.G.A. Aysheh, T. Khattab, and A. Massoud, "Cyber-attacks against voltage profile in smart distribution grids with highly-dispersed PV generators: detection and protection," *IEEE Electric Power and Energy Conference (EPEC)*, Edmonton, AB, Canada, 2020, pp. 1-6.

[13] A. Farroq, K. Shahid, Y. Gui, and R.L. Olsen, "Impact of cyber-attack on coordinated voltage control in low voltage grids," *IET Renew. Power Gener.*, vol 17, no. 11, pp. 2887-2894, Aug. 2023.

[14] A. Agrawal, D.M. Momin, D. Syndor, and S. Affijulla, "Impact analysis of cyber attack under stable state of power system: voltage stability," *IEEE Region 10 Symposium (TENSYMP)*, Dhaka, Bangladesh, 2020, pp. 402-405.

[15] H. Rahimpour, J. Tusek, A. Abuadbba, A. Seneviratne, T. Phung, A. Musleh, and B. Liu, "Cybersecurity challenges of power transformers," arXiv:2302.13161, Mar. 2023, doi: https: 10.48550/arXiv.2302.13161.

[16] D. Jin, H.-D. Chiang, and P. Li, "Two-timescale multi-objective coordinated volt/var optimization for active distribution networks," *IEEE Trans. Power Syst.*, vol. 34, no. 6, pp. 4418-4428, Nov. 2019.

[17] MATPOWER Package. [Online]. Available: https://matpower.org/.

[18] Wind-Turbine-Models (2023). https://en.wind-turbine-models.com/.

[19] A. Asrari, E. Naderi, J. Khazaei, P. Fajri, and V. Cecchi, "Modern heat and electricity incorporated networks targeted by coordinated cyberattacks for congestion and cascading outages," in *Coordinated Operation and Planning of Modern Heat and Electricity Incorporated Networks*, IEEE, Piscataway, NJ, USA, 2022.