False Data Injection Attack Targeting the LTC Transformers to Disrupt Smart Grid Operation

Adnan Anwar(✉), Abdun Naser Mahmood, and Mohiuddin Ahmed

School of Engineering and Information Technology, UNSW Canberra, Canberra, ACT 2600, Australia
adnan.anwar@adfa.edu.au, Abdun.Mahmood@unsw.edu.au, mohiuddin.ahmed@student.adfa.edu.au

Abstract. Load Tap Changing (LTC) Transformers are widely used in a Power Distribution System to regulate the voltage level within standard operational limit. In a SCADA connected network, the performance of LTC transformers can be improved by utilizing a closed loop monitoring and control mechanism. The widely used SCADA communication protocols, including Modbus and DNP3, have been proven vulnerable under cyber attack. In this paper, we conduct a vulnerability analysis of LTC transformers under malicious modification of measurement data. Here, we define two different attack strategies, (i)attack targeting energy system efficiency, and (ii) attack targeting energy system stability. With theoretical background and simulation results, we demonstrate that the attack strategies can significantly affect the power distribution system operations in terms of energy efficiency and stability. The experiments are performed considering IEEE benchmark 123 node test distribution system.

Keywords: False Data Injection · Smart grid FDI attacks · Cyber security · OpenDSS · LTC transformer

1 Introduction

Voltage stability has been identified as one of the major concerns of power distribution system planning and operation [1]. Traditionally, the power distribution system is designed such a way that the voltage continues to drop with the increase of the feeder length. At peak load or the heavily loaded conditions, the voltage drop phenomena may affect the distribution system stability significantly which can further lead to a voltage collapse situation [2]. Due to voltage stability or collapse problems, a large blackout may occur in a distribution system which can again lead to a cascading failure in the transmission system resulting huge customer sufferings and significant financial losses. In order to improve of voltage stability of a distribution system, Load Tap Changing (LTC) transformers are widely used which regulates the voltage profiles by changing the tap locations [3]. In a traditional setup, LTC transformers rely on the current and voltage measurement data which are obtained using the local information of that node

J. Tian et al. (Eds.): SecureComm 2014, Part II, LNICST 153, pp. 252–266, 2015.
DOI: 10.1007/978-3-319-23802-9_20

where LTC transformer is connected. Although this local measurement based LTC operation can control the voltage profile at a upstream node where LTC transformers are connected, still downstream nodes of a traditional radial distribution feeder may suffer from poor voltage magnitudes due to lack of observability of the total system. Hence, in a smart grid environment, the operation of the LTC transformers are improved by utilizing an End-of-Line (EoL) voltage feedback with the aid of remote monitoring devices (voltage sensors) and communication networks [4]. This closed loop adaptive voltage control method improves the overall voltage profiles and ensures Conservation Voltage Reduction (CVR) of a smart distribution grid but may introduce new security vulnerabilities as control signals are passed through a communication network. In an Advanced Metering Infrastructures (AMI) based Smart Grid environment, end-user measurement data from smart sensors may also be used to take the voltage control decisions which is again proven vulnerable to spoofing attacks or man-in-the-middle attacks, typically known as False Data Injection (FDI) attacks in the Smart Grid community. These *Data Integrity* attacks targeting the LTC transformers to disrupt the stable voltage operation will have two major consequences- (i) *failure or decrement of the lifetime of LTC transformers*, and (ii) *Service interruptions and system failures resulting poor customer reliability and huge financial loss.* In the following paragraphs, we discuss recent cyber related anomalies in different components and operational modules of a Smart Grid and then draw the connections of these new yet alarming FDI attacks on the LTC transformers which can be launched to disrupt the stable voltage operations.

1.1 Cyber Attacks on the Smart Grid

We classify the Smart Grid vulnerabilities into four broad classes, discussed below:

(i) Cyber Attacks on the Communication Channels: Smart Grid is a cyber-physical infrastructure where both communication networks and physical power grid are highly coupled. Under a Supervisory Control And Data Acquisition (SCADA) controlled Smart Grid environment, traditional communication protocols (e.g., Modbus, DNP3, etc.) are proven vulnerable to cyber attacks [5–7]. For example, vulnerability of Modbus protocols are discussed in [5], where authors also propose a bloom filter based Intrusion Detection System (IDS) to protect the field devices of a SCADA system. Queiroz et al. propose a Smart Grid simulator where they discuss a scenario considering Modbus attacks to disrupt the operations of a SCADA connected wind farm [6]. Vulnerabilities of DNP3 protocols are discussed in [7] where authors design firewalls based on the monitoring and analysis of the system states. A detailed surveys of the cyber security issues of the Smart Grid is discussed in [8].

(ii) Cyber Attacks on the Smart Grid Operational Modules: A good number of research works have been conducted on the security issues of the Smart

Grid operational modules. State estimator, which is an important tool for determining system states, may produce misleading operational decision under a FDI attack. Authors in [9] have developed some heuristic approaches that have been proven to be successful in attacking the DC state estimation in such a way so that the malicious changes in the data cannot be detected by the state estimation module, hence the attach remains undetected. Further enhancement of the work can be found in [10]. While the research work [9,10] focuses on how to develop these types of unidentifiable attack, other research work are related to the development of a defense model [11,12]. Databases of the Smart Grid operation centre are also vulnerable to cyber attacks. This database manipulation attack may be undetected if proper security actions are not taken, as discussed in [13,14].

(iii) Cyber Attacks on the Sensor Devices: By gaining the access of the sensors (e.g., Smart meters) and Intelligent Electronic Devices (IEDs), an intruder can inject or manipulate wrong information. Various threats of AMI devices are discussed in [16,17]. Authors in [16] propose an adaptive tree based method to identify the malicious meters in a Smart Grid. A hybrid IDS for theft detection of AMI smart meters is proposed by Lo et al. in [17].

(iv) Cyber Attacks on the Actuators of a Control Device: The Automatic Generation Control (AGC) utilizes the power flow and frequency measurement data obtained from the remote sensors to regulate the system frequency within a specified bound. Esfahani et al. discuss the cyber attack scenarios of the AGC devices from the attacker's point of view [18]. To defend against these types of attacks targeting AGC, a model-based attack detection and mitigation strategy is proposed by Sridhar et al. in [19]. A detailed discussion and review of different Smart Grid cyber attacks can be obtained from [20,21]

1.2 Contribution

Although significant research works have been conducted considering the above top three types of security issues, there is still enough opportunity to further investigate the impact of cyber attacks on different actuators in a physical Smart Grid. Hence, we consider the remote node monitoring capability based adaptive voltage control of a LTC transformer to analyse the impacts of the FDI attacks. Specifically, the contributions of this paper are as follows:

(1) First, we discuss the voltage drop phenomena of a typical power distribution system and then show how the LTC operations can improve the voltage profile of the system. Then, we investigate the impact of the remote monitoring facilities under a Smart Grid consideration and explore how it can further improve the voltage profile of the whole radial system by ensuring the observability of the most distant node from the LTC transformer.

(2) Finally, the operation of the LTC transformer is analysed under FDI attacks. With extensive experiments, we show that the FDI attacks on the measurement data of the LTC controller will decrease the system efficiency and

stability. To the best of our knowledge, this paper, for the first time considers the FDI attacks on the operation of a LTC transformer. Here, we define two different attack strategies where measurement data are maliciously manipulated such a way it decreases the system efficiency or stability. For example, if the downstream node voltages are very close to the minimum operational threshold and they need LTC operations to boost up the voltages, the measurement data are modified such a way that the LTC controller takes the decision to decrease the actuator taps further instead of boosting up. As a results, voltage profiles in the physical downstream nodes will go beyond the minimum threshold of voltage stability limit.

1.3 Organization

The organization of this paper is as follows- In Sect. 2, the voltage drop phenomena of a distribution system and the corresponding LTC operations for voltage regulations are discussed. Adaptive LTC control operation with remote node monitoring mechanism is discussed in Sect. 3. Our proposed attack definitions and their impacts on the LTC operations towards disrupting energy system operation is discussed in Sect. 4. The paper concludes with some brief remarks in Sect. 5.

2 Preliminaries

In this section, we explain the voltage drop phenomena of a typical radial power distribution system. Then the construction and operational procedures of a LTC transformer based on local measurement data is discussed.

2.1 Voltage Drop of a Power Distribution System

Voltage stability has been a subject of great interest in recent years in attempts to ensure secure power system operations [22]. It refers to the ability of a power system to maintain steady voltages at all its nodes when there is a progressive or uncontrollable drop in its voltage magnitude after a disturbance, increase in load demand or change in operating conditions [23]. Voltage instability can lead to a voltage collapse which can be defined as a point in time at which the voltage becomes uncontrollable after a voltage instability [2]. Two major symptoms of voltage collapse are a low voltage profile and inadequate reactive power support. Generally, a distribution system is a low-voltage network which is very prone to the voltage collapse phenomena when it experiences increases in its load demand. Traditionally, distribution networks have been modelled for power delivery and consumption as a passive network considering the voltage drop phenomena. Actually, the R/X ratio of a transmission system is very low but, as the resistance of the conductors in a distribution system is very high, this leads to voltage drops along the distribution lines from the substation to load

centre. To exemplify the effect of voltage drop, we consider IEEE benchmark 123 node test distribution system [24]. Under peak load condition, the voltage profiles of *phase-A* of the 123 node test system is plotted in the Fig. 1 using the sign 'o'. In the current setup we show the voltage drop phenomena without considering any LTC control. As seen from the figure, a good number of downstream nodes are below the minimum voltage stability threshold.

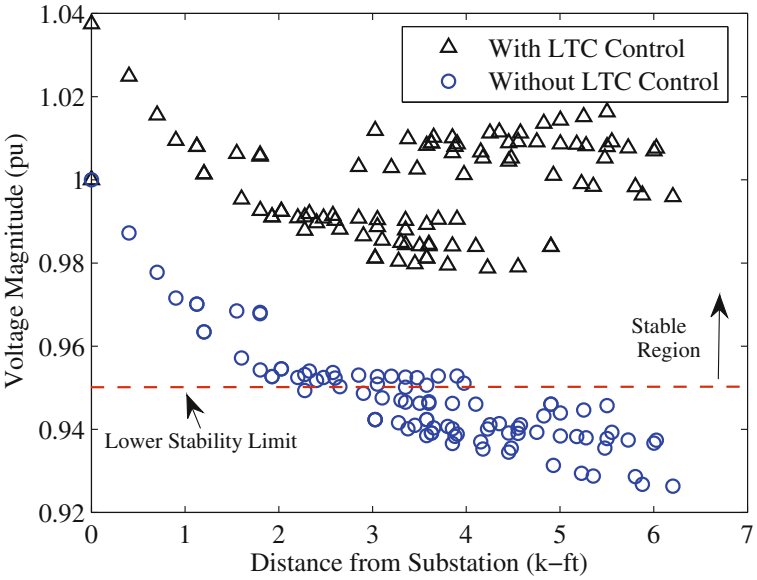

Fig. 1. Voltage profile of 123 node test system with and without LTC control

2.2 LTC Operation

In order to improve the voltage profile of downstream nodes, voltage regulation mechanism can be used. Traditionally, voltage regulation is performed based on an autotransformer with LTC mechanism. The desired voltage level is obtained by changing the taps of the series windings of the autotransformer [25]. The decision of the position of the desired tap is determined using a control circuit equipped with Line Drop Compensator (LDC). Generally, there are 32 taps in an LTC transformer and each tap changes the voltages by 0.00625 pu on a 120 V base [25]. Throughout the operation of the LTC transformers, ANSI/IEEE C57.15 standard is maintained to limit the voltage within the voltage stability ratings. The operations blocks of the LTC transformer is shown in Fig. 2.

We simulate the impact of LTC operation on the voltage profile of IEEE 123 node test system. The parameter settings of the LTC transformer and their

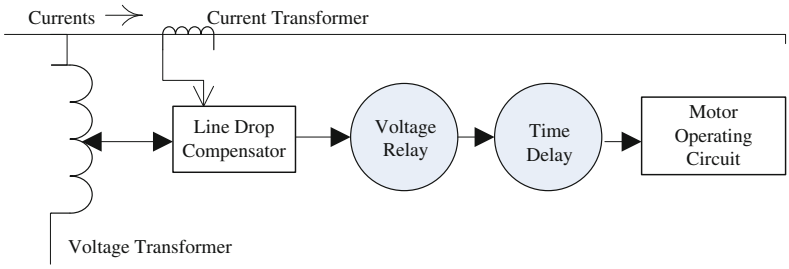

Fig. 2. LTC transformer block used for voltage regulation [25]

definitions are given in the Appendix. Using four LTC transformers, we obtain the voltage profile that maintain ANSI/IEEE C57.15 standard and remain within the stability margin. The *phase-A* voltage magnitudes are plotted in the Fig. 1 using the sign '△'

3 Adaptive LTC Controller with Remote Monitoring Capabilities

In a traditional setup, the control decision of a LTC transformer is processed based on the local measurements of currents and voltages. As a result, the optimal control decision is not possible as the *Voltage Control Processor (VCP)* lacks full observability of the distribution system. Typically, the distribution systems are radial in nature where the voltage drops gradually and the *EoL* node faces the maximum voltage deviations. Therefore, monitoring the *EoL* node, the performance of the LTC operations can be further improved. In a Smart Grid, the

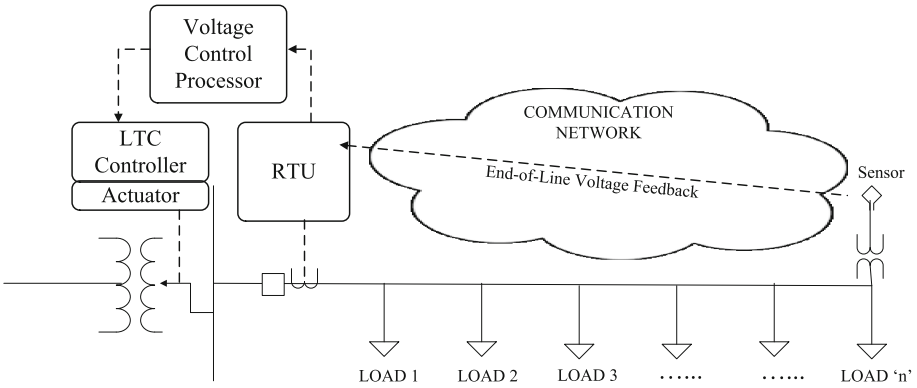

Fig. 3. Operational diagram of an adaptive LTC controller

sensor connected with the *EoL* node sends the measurement data or control input through a communication channel to the Intelligent Electronic Devices (IEDs) connected with the LTC transformers. The VCP within the IED takes intelligent decisions based on the input data. This is a *closed loop* process which takes adaptive control decisions based on the change of the input measurements. An operational diagram of this adaptive LTC control technique is given in Fig. 3.

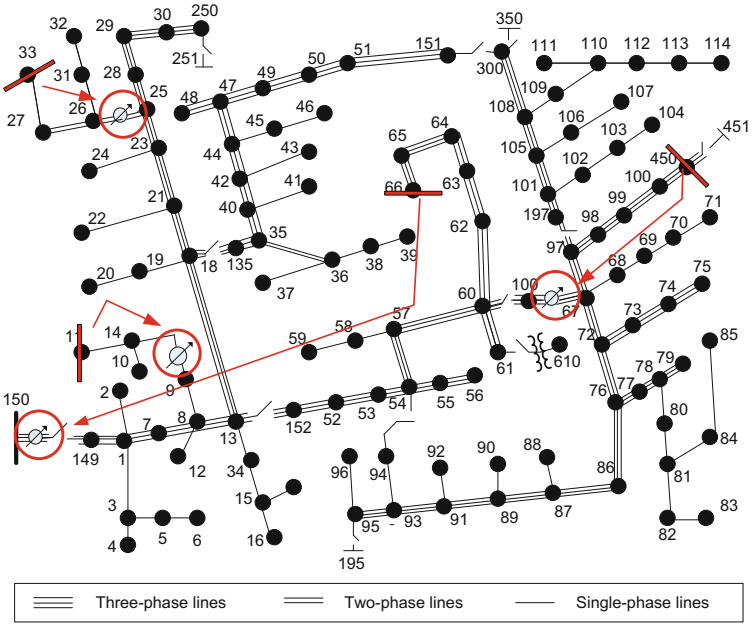

Fig. 4. LTC transformer locations and their corresponding remote monitoring node. Here, the *red circle* represents the LTC transformers and the *red* marked nodes are the remote nodes being monitored and controlled (Color figure online).

To simulate the impact of the adaptive LTC controller on the voltage profile, we consider a typical load profile of 24-hr period obtained from [26]. We run the power flow using Electric Power Research Institutes's (EPRI) OpenDSS [26] for the 24-hr period considering local measurement based LTC operations following the parameter settings described in the Appendix. For the same load profile, we use adaptive LTC operations using remote monitoring of node voltages. Therefore, the monitoring buses are set following the Fig. 4, where the target voltage of remote controlled node is set to 116 V with a 2 V bandwidth. Here, the remote nodes are being monitored by the LTC controller in the IED and control decisions are taken accordingly to run the system in a lower voltage level, which is welly known as CVR. Due to this adaptive LTC operations with measurement data feedback, the system efficiency is increased upto 1.8 % and an average of 1.4 % as shown in Fig. 5.

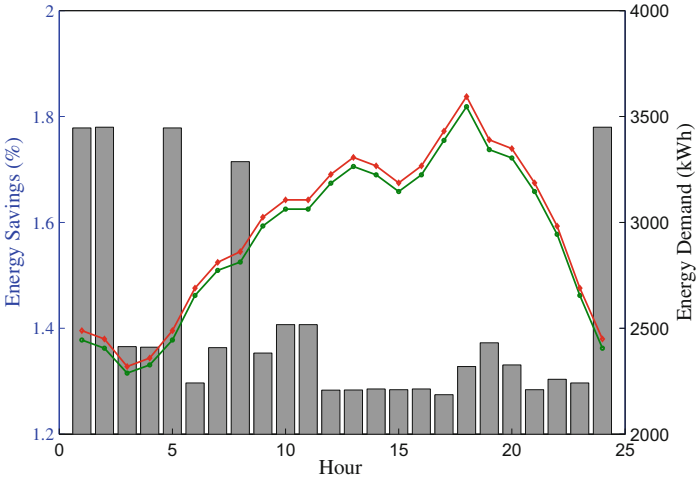

Fig. 5. Energy savings in a typical day using adaptive LTC transformers

4 FDI Attacks: Constructions and Impact

Although this remote monitoring based adaptive LTC control increases the efficiency, they introduce new vulnerabilities. In a SCADA connected network, sensors and actuator communicate with each other using Modbus, DNP3 or IEC 61850 standard protocols. The Modbus, DNP3 has already proven vulnerable under different types of cyber attacks, e.g., spoofing attacks [5–7]. Besides, with the advancement of Smart Grid, LTC operations can be further improved using closed loop measurement feedback from AMI smart meters. Widespread use of smart meters need the use of TCP/IP protocols, which is again vulnerable to cyber attacks [27,28]. In Fig. 6, the closed loop operation of adaptive LTC control under the attack uncertainty is shown.

In our analysis, we demonstrate two different types of attack strategies, discussed below:

(i) ***Attacking Energy Efficiency:*** Attacker maliciously modify the voltage measurement data such a way that the system operates at a higher voltage level which will need more power supply from the substation. As a result, it will increase cost and decrease the system efficiency as more energy is needed under an attack scenario compared with the base case. One simple example is demonstrated to illustrate the scenario. Suppose, the base voltage of the LTC is set to 120 V with a bandwidth of 2 V ($120 \pm 1V$). As the LTC has 32 taps, around 0.75 V change occurs due to per tap change [25]. Now we consider a situation where monitored node voltage is below the minimum voltage regulation limit of the LTC ($120V - 1V$). Therefore, the desired number of *tap operation* the LTC needs to control, can be calculated as follows:

$$Number\ of\ tap\ change,\quad k_t^a = \frac{V_{reg}^{low} - V_{meas}}{\Delta V_{tap}} \tag{1}$$

here, $V_{reg}^{low} = 119\ V$ and $\Delta V_{tap} = 0.75$. For any measurement voltage, $V_{meas} = 114.6\ V$, the LTC needs the following tap operations:

$$k_t^a = \frac{119 - 114.6}{0.75} = +5.47 \approx +6\ taps \tag{2}$$

here, '+' sign indicates that the actuator will increase the tap and approximation to 6 is made as tap number must be an integer value. Now, if the measurement voltage information V_{meas} is manipulated such a way that the original measurement values are decreased (e.g.,$V_{FDI} < V_{meas}$), the required number of tap operations will be increased following the Eq. (1). For example, if the LTC controller receive the measurement value $V_{FDI} = 112V$ instead of the true measurement value $V_{meas} = 114.6V$, the required number of tap operations will be calculated as $k_t = 14$. As the manipulated measurement information V_{FDI} does not represent the actual quantity of voltage (note, the true value is V_{meas}), the overall system will be operated at a higher voltage level due to the increase of tap operations. As the aim of the CVR is to lower the voltage level (by maintaining the standard stability limit) to increase the efficiency, operation at a higher voltage level will violate the CVR principles, hence the system efficiency will be degraded.

Based on the above discussions, we define the attack model towards energy inefficiency as follows:

$$V_{FDI}(t) = \begin{cases} V_{reg} - \Delta V_{tap} * k_t^a(t), & if\ no\ attack \\ V_{reg} - \Delta V_{tap} * k_t^m(t), & if\ attack\ exists \end{cases} \tag{3}$$

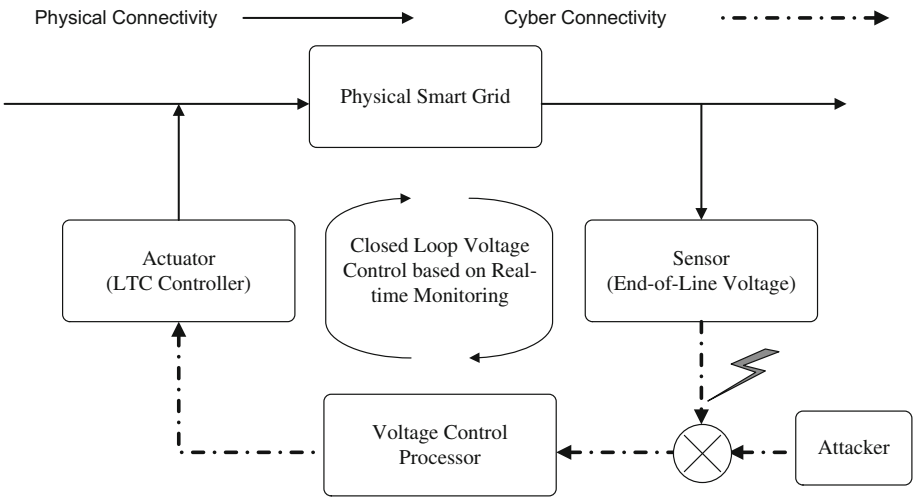

Fig. 6. Closed loop voltage control based on real-time monitoring

s.t.,

$$k_t^{max} > k_t^m(t) > k_t^a(t)$$

here, $k_t^m(t)$ is the intended number of tap operations chosen by the attacker and k_t^{max} is the maximum number of tap operations possible by the LTC transformer (generally, k_t^{max}=16 in one direction). Other symbols have their usual meaning defined above. Any value of $k_t^m(t)$ that is greater than k_t^a will represent a malicious modification of the measurement data which will initiative an attack scenario. The maximum value of $k_t^m(t)$ must not exceed the maximum possible tap operation value. Any value of $k_t^m(t)$ that is equal to k_t^a will produce the same corrupted measurement equal to the original measurement (hence, it does not represent an attack scenario). Note, all the values of k_t^{max}, $k_t^m(t)$, and k_t^a are integer as number of taps can't be a fraction. A larger value of k_t^a represents a greater attack magnitudes in terms of energy inefficiency.

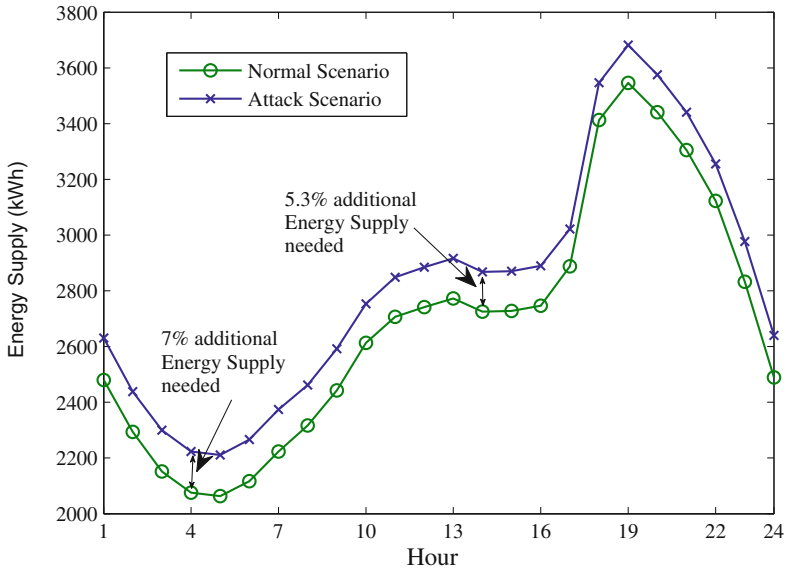

Fig. 7. Attack targeting energy system efficiency

Based on the load data, first we simulate the LTC operations with remote node voltage monitoring facilities using OpenDSS. Then, the corrupted measurements are generated following the Eq. (3), considering $k_t^m(t) = +8$. The total power supplied by the substation under normal situation and attacked scenario is plotted in Fig. 7. After the attack, we see that the total amount of energy supply is increased significantly, which is around 5.5 % in an average and maximum 7 % increase of the normal case. As the operational cost is a quadratic function of supply energy, the overall operational cost of the system will increase due to

the need of the additional energy resulting from the attack vectors. Hence, the system efficiency will decrease significantly.

(i) ***Attacking Energy Stability:*** Now we recall the examples and the procedures of calculating desired tap value from the measurement data discussed in the previous section. If the measurement voltage is 114.6 V, the LTC controller takes the decision to increase the tap positions by 6 steps as calculated in Eqs. (1) and (2). Now, we observe that the measurement value V_{meas} is already at the lower half of the stability region, hence, the corresponding node voltage needs to be boost up by the LTC operations. However, if the LTC tap positions are further decreased rather than boosting up, the downstream node voltages of the LTC will decrease further which may go beyond the minimum voltage stability limit recommended by ANSI/IEEE. As a result, voltage collapse and system instability may occur resulting poor reliability of the system. So, the attacker may wish to target the system stability and reliability by maliciously manipulating the voltage measurement information such a way that it further decrease the LTC taps. Therefore, the attacker may utilize the relation of voltage measurements and tap numbers described in Eq. (4) to take intelligent decisions to disrupt the voltage stability of the system. Based on the above discussions, we define the attack model to unstable the system as follows:

$$V_{FDI}(t) = V_{reg} + \Delta V_{tap} * \lambda(t) \tag{4}$$

where,

$$\lambda(t) \in [+1, +16] \quad and \quad \lambda(t) > k_t^a(t) \tag{5}$$

here, $\lambda(t)$ is an attack factor defined using Eq. (5). For the value of $\lambda = 0$, $V_{FDI} = V_{meas} = V_{reg}$, therefore, the LTC controller calculates the value of $k_t^a = 0$ using Eq. (1). For the above example, where the measurement voltage is 114.6 V, the value of k_t^a is +6 obtained from the Eqs. (1) and (2). Now, following the attack definition in Eq. (4), we consider $\lambda = +8$ which is obviously greater than the calculated k_t^a=+6. Therefore, the attacker can modify the original measurement voltage with the new V_{FDI} which is 127 V. Once the LTC controller receives the measurement data (which is actually maliciously modified), it calculates the expected number of tap operations following below:

$$k_t^a(t) = \frac{V_{reg}^{up} - V_{meas}}{\Delta V_{tap}} = \frac{121 - 127}{0.75} = -8 \tag{6}$$

After the tap number is calculated, the actuator decreases 8 taps (downwards) to decrease the voltage level. As the original voltage was only 114.6 V, further decrement will force the node voltage to remain below the stability limit as shown in Fig. 8.

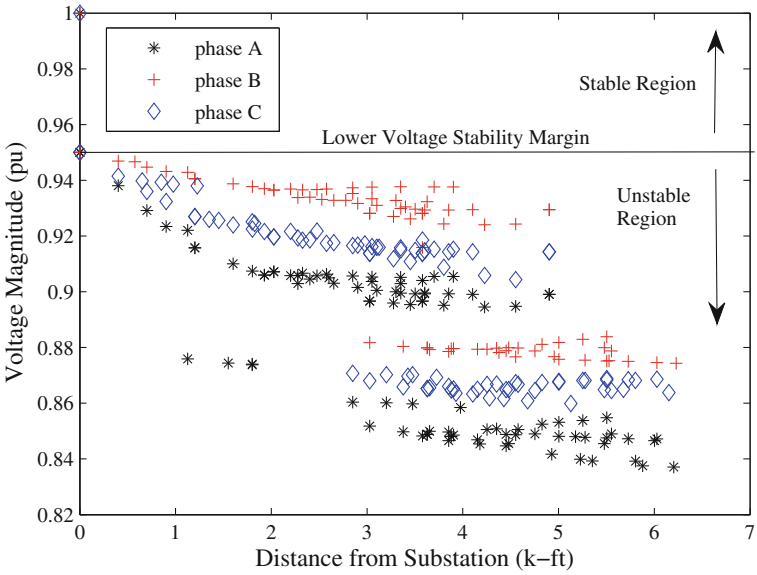

Fig. 8. Attack targeting energy system stability

5 Conclusion

In this paper, we have discussed the voltage drop phenomena of a traditional distribution system and the effect of LTC transformers to regulate the voltage level within stability margin. The advantages of closed loop adaptive LTC control based on the remote node monitoring is also explained. As the operation the this closed loop LTC control is highly dependent on the measurement data from a remote node, we show how the malicious modification (*FDI attacks*) of the measurement data can lead to distribution system operational disruptions. Here, we define two different types of attacks, one aiming to decrease the energy efficiency by demanding additional power from the substation and the another one is targeting the system stability by forcefully placing all node voltages under the lower stability margin. For the first type of attack, we see that a typical attack scenario can increase the need of power supply by 7 %. For the second attack type, every node of the distribution system goes below the stability threshold under a typical attack situation.

The scope of this paper is to define and study these new attack templates that target the LTC transformers to disrupt distribution system operations from an attacker's perspective. An Intrusion Detection System (IDS) to defend against these types of attacks is under preparation.

6 Appendix

Regulator ID:	1
Line Segment:	150 - 149
Location:	150
Phases:	A-B-C
Connection:	3-Ph, Wye
Monitoring Phase:	A
Bandwidth:	2.0 volts
PT Ratio:	20
Primary CT Rating:	700
Compensator:	Ph-A
R - Setting:	3
X - Setting:	7.5
Voltage Level:	120

Regulator ID:	2
Line Segment:	9 - 14
Location:	9
Phases:	A
Connection:	1-Ph, L-G
Monitoring Phase:	A
Bandwidth:	2.0 volts
PT Ratio:	20
Primary CT Rating:	50
Compensator:	Ph-A
R - Setting:	0.4
X - Setting:	0.4
Voltage Level:	120

Regulator ID:	3	
Line Segment:	25 - 26	
Location:	25	
Phases:	A-C	
Connection:	2-Ph, L-G	
Monitoring Phase:	A-C	
Bandwidth:	1 volts	
PT Ratio:	20	
Primary CT Rating:	50	
Compensator:	Ph-A	Ph-C
R - Setting:	0.4	0.4
X - Setting:	0.4	0.4
Voltage Level:	120	120

Regulator ID:	4		
Line Segment:	160 - 67		
Location:	160		
Phases:	A-B-C		
Connection:	3-Ph, L-G		
Monitoring Phase:	A-B-C		
Bandwidth:	2 volts		
PT Ratio:	20		
Primary CT Rating:	300		
Compensator:	Ph-A	Ph-B	Ph-C
R - Setting:	0.6	1.4	0.2
X - Setting:	1.3	2.6	1.4
Voltage Level:	124	124	124

References

1. Roy, N.K., Pota, H.R., Anwar, A.: A new approach for wind and solar type DG placement in power distribution networks to enhance systems stability. In: 2012 IEEE International Power Engineering and Optimization Conference (PEOCO), Melaka, Malaysia, 6–7 June 2012, pp. 296–301 (2012)
2. Johansson, S., Sjogren, F.: Voltage collapse in power systems, Ph.D. thesis, Chalmers University of Technology (1995)
3. Dzafic, I., Jabr, R.A., Halilovic, E., Pal, B.C.: A sensitivity approach to model local voltage controllers in distribution networks. IEEE Trans. Power Syst. **29**(3), 1419–1428 (2014)
4. Uluski, R.W.: VVC in the smart grid era. IEEE Power Energy Soc. Gen. Meet. **2010**, 25–29 (2010)
5. Parthasarathy, S.; Kundur, D.: Bloom filter based intrusion detection for smart grid SCADA. In: 25th IEEE Canadian Conference on Electrical & Computer Engineering (CCECE), pp. 1–6 (2012)
6. Queiroz, C., Mahmood, A., Tari, Z.: SCADASim - a framework for building SCADA simulations. IEEE Trans. Smart Grid **2**(4), 589–597 (2011)

7. Fovino, I.N., Coletta, A., Carcano, A., Masera, M.: Critical state-based filtering system for securing SCADA network protocols. IEEE Trans. Ind. Electron. **59**(10), 3943–3950 (2012)
8. Wang, Wenye, Zhuo, Lu: Cyber security in the smart grid: survey and challenges. Comput. Netw. **57**, 1344–1371 (2013)
9. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 21–32. ACM (2009)
10. Ozay, M., Esnaola, I., Vural, F., Kulkarni, S., Poor, H.: Sparse attack construction and state estimation in the smart grid: centralized and distributed models. IEEE J. Sel. Areas Commun. **31**, 1306–1318 (2013)
11. Hug, G., Giampapa, J.: Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. IEEE Trans. Smart Grid **3**, 1362–1370 (2012)
12. Qin, Z., Li, Q., Chuah, M.-C.: Defending against unidentifiable attacks in electric power grids. IEEE Trans. Parallel Distrib. Syst. **24**, 1961–1971 (2013)
13. Valenzuela, J., Wang, J., Bissinger, N.: Real-time intrusion detection in power system operations. IEEE Trans. Power Syst. **28**, 1052–1062 (2013)
14. Mousavian, S., Valenzuela, J., Wang, J.: Real-time data reassurance in electrical power systems based on artificial neural networks. Electr. Power Syst. Res. **96**, 285–295 (2013)
15. Grochocki, D.; Huh, J.H.; Berthier, R.; Bobba, R.; Sanders, W.H.; Cardenas, A.A.; Jetcheva, J.G.: AMI threats, intrusion detection requirements and deployment recommendations. In: IEEE Third International Conference on Smart Grid Communications (SmartGridComm), 5–8 November 2012, pp. 395–400 (2012)
16. Xiao, Z., Xiao, Y., Du, D.H.: Exploring malicious meter inspection in neighborhood area smart grids. IEEE Trans. Smart Grid **4**(1), 214–226 (2013)
17. Lo, C.-H., Ansari, N.: CONSUMER: a novel hybrid intrusion detection system for distribution networks in smart grid. IEEE Trans. Emerg. Top. Comput. **1**(1), 33–44 (2013)
18. Esfahani, P.M., Vrakopoulou, M., Margellos, K., Lygeros, J., Andersson, G.: A robust policy for automatic generation control cyber attack in two area power network. In: 49th IEEE Conference on Decision and Control (CDC) (2010)
19. Sridhar, S., Govindarasu, M.: Model-based attack detection and mitigation for automatic generation control. IEEE Trans. Smart Grid **5**(2), 580–591 (2014)
20. Anwar, A.; Mahmood, A.: Cyber security of smart grid infrastructure. In: The State of the Art in Intrusion Prevention and Detection, CRC Press, USA, 2014, CRC Press, Taylor & Francis Group, pp. 139–154
21. Anwar, A., Mahmood, A.: Vulnerabilities of smart grid state estimation against false data injection attack. In: Hossain, J., Mahmud, A. (eds.) Renewable Energy Integration. Green Energy and Technology, pp. 411–428. Springer, Singapore (2014)
22. Yorino, N., Sasaki, H., Masuda, Y., Tamura, Y., Kitagawa, M., Oshimo, A.: An investigation of voltage instability problems. IEEE Trans. Power Syst. **7**, 600–611 (1992)
23. Kundur, P., Paserba, J., Ajjarapu, V., Andersson, G., Bose, A., Canizares, C., Hatziargyriou, N., Hill, D., Stankovic, A., Taylor, C., Van Cutsem, T., Vittal, V.: Definition and classification of power system stability - IEEE/CIGRE joint task force on stability terms and definitions. IEEE Trans. Power Syst. **19**, 1387–1401 (2004)

24. Distribution System Analysis Subcommittee Radial Test Feeders. http://ewh.ieee.org/soc/pes/dsacom/testfeeders/index.html
25. Kersting, W.: Distribution System Modeling and Analysis. CRC Press, Boca Raton (2002)
26. Smart Grid Resource Center, Simulation Tool OpenDSS. http://www.smartgrid.epri.com/SimulationTool.aspx
27. Liu, C.-C., Stefanov, A., Hong, J., Panciatici, P.: Intruders in the grid. IEEE Power Energy Mag. **10**(1), 58–66 (2012)
28. Xie, Y., Yu, S.-Z.: A large-scale hidden semi-markov model for anomaly detection on user browsing behaviors. IEEE/ACM Trans. Netw. **17**(1), 54–65 (2009)