Transient Model-Based Detection Scheme for False Data Injection Attacks in Microgrids

James Ranjith Kumar R.*, Deepa Kundur†, Biplab Sikdar*
*Department of Electrical and Computer Engineering
National University of Singapore
Email: jamesranjithkumar@u.nus.edu, bsikdar@nus.edu.sg
†Department of Electrical and Computer Engineering
University of Toronto
Email: dkundur@ece.utoronto.ca

***Abstract*—Centralized controllers are popularly used in Microgrid as it ensures its economic and stable operation. The measurements taken for such a controller are prone to false data injection (FDI) attacks which may result in destabilizing the microgrid. This paper presents a technique that uses transient information for detecting the FDI attacks in a microgrid. The detection technique works on the principle that any legitimate change in the system will be accompanied by a transient that can be observed by the measurement system. The transient solution is obtained using a backward forward sweep technique which is developed in this paper. This technique is much efficient than the Electromagnetic Transient Program (EMTP) as it solves the dynamic equations by exploiting the radial feature of the microgrid network. The solution is compared against the measured values such that in the event of an FDI attack, transients may not be present and hence it will have high deviations. The proposed technique is evaluated on a microgrid under the FDI attack and the results are presented.**

***Index Terms*—Microgrid, False Data Injection Attack, Smart Grid, SCADA, Transients, EMTP**

I. Introduction

One of the motivations for having a microgrid in any establishment is to have a secure uninterrupted power supply [1]. This is due to the characteristic of the micro grid that it can maintain the power supply in both grid connected and islanded mode. Microgrids are often powered by a multiple of Distributed Energy Resources (DER) instead of a single source in order to be self sufficient in islanded mode. Centralized control for such DERs are usually adopted for islanded micro grids as the network structure remains unchanged [2]. The function of central microgrid controller is to provide control signals to DERs such that its operation is economical and reliable. For decision making process, the central controller utilizes the measurement values taken across various points of the microgrid and transported through the communication network. Due to the closeness between the generation and load, any slight imbalance in the power flow may lead to extreme frequency fluctuations. Hence any cyber attack on the microgrid controller can lead to a immediate collapse of the stability of the system.

There has been tremendous interest in the recent years in the study of FDI attacks specifically on transmission side of power system. Stealthy FDI attacks was first introduced in [3] where it is shown that the output of the state estimator can be manipulated using the information of the transmission network. In this work, it has been shown that, the traditional bad data detection techniques can be bypassed when the attack vector is the linear combination of the gain matrix. The studies on stealthy FDI attacks can be categorized as: analyzing the effects on power grid, detection techniques for FDI attacks and reinforcement of the security of the grid. The studies that has been done for transmission system may not be directly applicable to distribution system especially microgrids because of its special features such as:

1) Network topology is mostly radial in nature
2) The feeders have high R/X ratio
3) The phase angle of voltages are small
4) Closely tied generations and loads

Similar to transmission system, microgrids are also vulnerable to stealthy FDI attacks where the operation of the central controller is usually the targeted. The vulnerabilities and potential threats in a microgrid are listed in [4]. The access points for cyber attacks on smart grid can happen at the DER terminals or at the communication channel or the microgrid grid controller itself [5]. It has been shown in [6] that the delay in measurements over the communication channel can have a significant effect on the microgrid operation. Zhang et al. [7] has demonstrated that FDI attacks has the ability to disrupt the partition process to form islanded microgrids. In [8], recursive systematic convolutional code based technique was proposed to add redundancy which act as a defense against FDI attacks in microgrid. Chlela et al. [9] had demonstrated the effects of FDI attacks on the active power flow and frequency of the microgrid. A FDI attack detection scheme was proposed in [10] for DC microgrid by identifying the changes in the selected candidate invariants. In [11], a trust based control protocol has been designed in order to protect the communication links of the microgrid controllers against data

This research is supported by the National Research Foundation, Prime Minister's Office, Singapore under its Corporate Laboratory@University Scheme, National University of Singapore, and Singapore Telecommunications Ltd.

manipulation attacks. A FDI attack model has been developed in [12] considering on the AMI infrastructure in a microgrid environment. A detailed study on the effect of FDI attacks in inverter based microgrid has been conducted in [13]. In this study, it is considered that the nodal information are exchanged with its adjacent nodes and even under this consideration, FDI attack can able to have a tremendous impact on voltage and frequency.

This paper focuses on developing computation algorithm which computes the microgrid transients and later compared against the measurements to identify the presence of FDI attacks. In this algorithm, the governing equations of the various elements of microgrid is simplified using the trapezoidal rule of integration. These algebraic equations are solved using a backward forward sweep technique that exploits the radial nature of the microgrid. Since FDI attacks target the steady state values of the measurements, the dynamics in those measurements are absent. Hence by the difference between the calculated values using the proposed algorithm and the measured values will be high during the transient period and the presence of attack can be detected.

The remainder of this paper is as follows: the second section gives a background of false data injection attacks. which is followed by the detailed description of the proposed method. After that, the results obtained using the proposed method in 5-bus system has been presented. Finally we conclude this paper with the future direction of this work.

II. Conventional EMTP models

. Electomagnetic transient program (EMTP) simulates the transient phenomenon of the electrical network with discrete time steps rather than continuously. This technique was initially proposed [14] and it later popularly used in a variety of transient simulators for power system networks. EMTP utilizes the trapezoidal rule of integration to solve the differential equations which govern the electrical network. The elements in a microgrid, such as the feeders, DERs, transformers and load can be modeled as interconnections of resistances, inductances and capacitances. This section specifically focus on the EMTP models for these linear lumped elements which are used in the proposed FDI attack detection scheme for microgrids. For each of the EMTP model, time is considered in discrete steps with each step of Δt width.

A. Resistance

Resistive elements are the part of equivalent circuit for DERs, transformers, feeders and loads. Switching elements such as circuit breakers are represented in form of variable resistance which has highest value on open state and negligible value on closed position. The EMTP model for a resistance with value R at time step k can be given as

$$i_R^k = \frac{1}{R}\left(v_{Ra}^k - v_{Rb}^k\right) \tag{1}$$

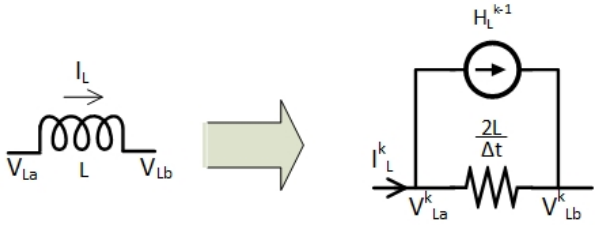


Fig. 1: EMTP model of Inductance.

B. Inductance

The effect of magnetic linkages due to the current flow in the conductors can be modeled as coupled and uncoupled inductances. In addition to resistance, inductance are also prevalent in the equivalent circuits of the microgrid elements. Consider an inductor L as shown in Fig.1 with its terminal voltages V_{La} and V_{Lb} respectively and the current flow in the inductor be I_L. The governing differential equation can be written as

$$V_{La} - V_{Lb} = \frac{dI_L}{dt} \tag{2}$$

At time step k, using the trapezoidal rule of integration, it can be simplified as

$$i_L^k = i_L^{k-1} + \frac{\Delta t}{2L}\left(V_{La}^k - V_{Lb}^k + V_{La}^{k-1} - V_{Lb}^{k-1}\right) \tag{3}$$

By simple algebraic manipulations, it can be written as

$$i_L^k = \frac{\Delta t}{2L}\left(V_{La}^k - V_{Lb}^k\right) + H_L^{k-1} \tag{4}$$

where

$$H_L^{k-1} = i_L^{k-1} + \frac{\Delta t}{2L}\left(V_{La}^k - V_{Lb}^k\right) \tag{5}$$

Thus the EMTP model of an inductance can be given as resistance of value $\frac{2L}{\Delta t}$ parallel to current source H_L^{k-1} as shown in Fig.1. This current source H_L^{k-1} caries the information of the previous time step as given in (5).

C. Capacitance

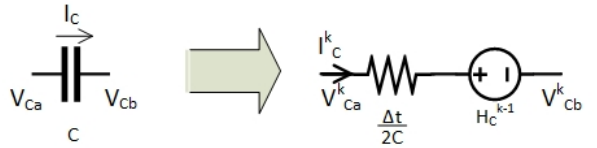


Fig. 2: EMTP model of Capacitance.

Lumped capacitance are modeled in order to account the effect of electric charge that trapped in the dielectrics at various elements of the electric network. The capacitance values may not be prominent in overhead feeders in a microgrid as these feeders are short but it has significant presence in the underground cable. Capacitance is also an essential component in of various reactive power compensators which are used in

the microgrid. For the obtaining the EMTP model, consider a capacitance C as shown in Fig. 2. Let V_{Ca} and V_{Cb} be the voltage at the capacitor terminals and I_C be the current flowing in the capacitor. The relation between the voltage and the current flow in a capacitor can be given as

$$V_{Ca} - V_{Cb} = \int I_C \, dt \tag{6}$$

By applying the trapezoidal rule of integration at time step k, it is simplified into algebraic form as

$$V_{Ca}^k - V_{Cb}^k = V_{Ca}^{k-1} - V_{Cb}^{k-1} + \frac{\Delta t}{2C}\left(I_C^k + I_C^{k-1}\right) \tag{7}$$

By further rearrangements, it can be

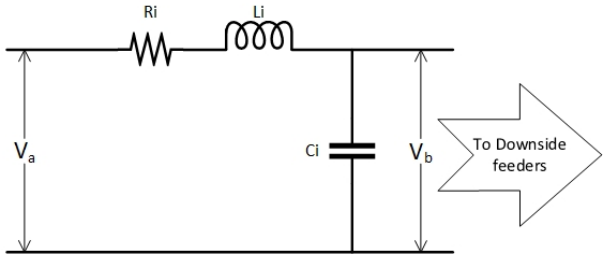
$$V_{Ca}^k - V_{Cb}^k = \frac{\Delta t}{2C} I_C^k + H_C^{k-1} \tag{8}$$

where

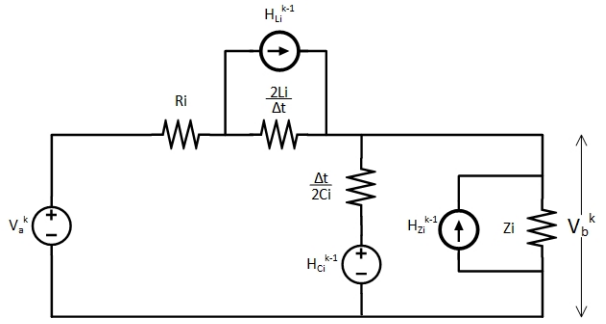
$$H_C^{k-1} = V_{Ca}^{k-1} - V_{Cb}^{k-1} + \frac{\Delta t}{2C} I_C^{k-1} \tag{9}$$

The discrete equivalent of capacitor at time step k can be given as a resistance of value $\frac{\Delta t}{2C}$ in series to a voltage source H_C^{k-1} as shown in Fig. 2. The information of the previous time steps are accounted with the voltage source H_C^{k-1} which is updated with (9) in every time step.

III. Solution for EMTP in Radial Networks



(a) Feeder Section



(b) EMTP Model equivalent

Fig. 3: Incorporating EMTP model in BFS algorithm

In most of the EMTP packages which is available transmission systems, the discretized models of the elements in the electric network were solved with a conventional tools available in Linear Algebra. Such solution technique may not be computational optimal for distribution system especially microgrids as they have radial structure. In [15], it has been shown that the load flow solution for a distribution network can be obtained effectively than the conventional techniques by exploiting its radiality. It is achieved by using a two part algorithm, where in the first part, the backward sweep accumulates the value of line flows and in the second part, the forward sweep computes the steady state voltage values. This section develops a similar strategy of backward-forward sweep (BFS) technique in order to solve the EMTP problem for radial system.

A. Feeder Modeling

Consider a feeder section i of a radial system as shown in Fig. 3a with V_a and V_b be the voltages at terminals a and b respectively. The radial network can be formed in a hierarchical structure, where from a root node, various leaf nodes radiate in a layer manner as shown in Fig. 4. In this feeder i, terminal a is a top level node and points towards root node and terminal b is a bottom level node and lies towards the downside feeders at the lower layers. At time step k, this feeder can be transformed into a discrete form using EMTP models as shown in Fig. 3b. In this equivalent network, Z_i and H_{Zi}^{k-1} represents equivalent resistance and the current injection of all the loads and feeders lie below feeder i. The feeder section i can be simplified into norton's equivalent from terminal a prospective, which is a thevenin's resistance Z_i^{th} in parallel to a current source $\mathcal{I}_i^k$. With simple algebraic computations, the equivalent thevenin's resistance can be written as

$$Z_i^{th} = R_i + \frac{2L_i}{\Delta t} + Z_i^{sh} \tag{10}$$

where

$$Z_i^{sh} = \frac{Z_i \frac{\Delta t}{2C_i}}{Z_i + \frac{\Delta t}{2C_i}} \tag{11}$$

Similarly the value of current source in the norton equivalent can be computed as

$$\mathcal{I}_i^k = \frac{Z_i^{sh} \mathcal{J}_i^k - \frac{2L_i}{\Delta t} H_{Li}^{k-1}}{Z_i^{th}} \tag{12}$$

where

$$\mathcal{J}_i^k = \frac{2C_i}{\Delta t} H_{Ci}^{k-1} - H_{Zi}^{k-1} \tag{13}$$

With this simplification, it has become easy to incorporate this model into the BFs algorithm. This values of resistance and current are accumulated from the bottom most node to the top level in a sequential manner which is popularly termed as backward sweep. In the same sequence, from top to bottom manner, the voltage at the terminal ends can be calculated from this equivalent circuit for each feeder. These can be termed as forward sweep as it does the computation starts from the root node and forwards towards the end of the radial system.

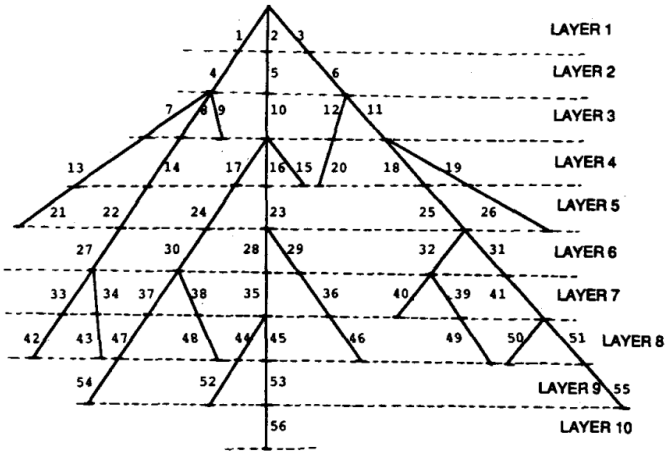


Fig. 4: Illustration of Node Numbering scheme [15].

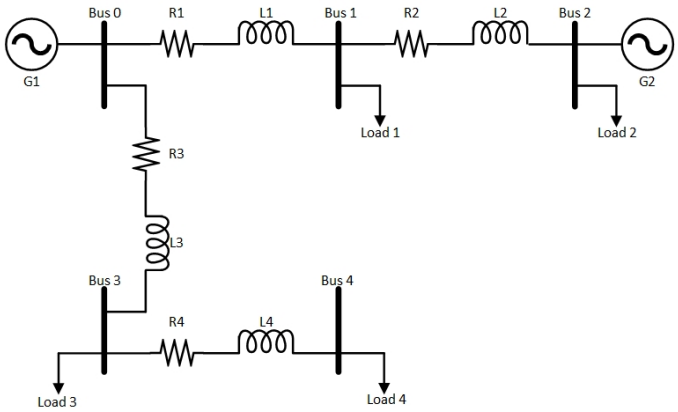


Fig. 5: 5-bus Radial Microgrid.

TABLE I: Feeder Data for 5-bus microgrid.

Top Bus	Bottom Bus	Line Parameters		Load at the bottom bus	
		R (mΩ)	L (mH)	Active Power (kW)	Reactive Power (kVAr)
0	1	96.3	12.45	-	-
1	2	64.2	8.3	3.6	2.7
0	3	44.94	5.81	3.6	2.7
3	4	96.3	12.45	3.6	2.7

B. Node Numbering Scheme

For the correct sequence of computation in backward and forward sweeps, it is important to order the terminals so that in any feeder, the computation of top node have been already done before proceeding to the bottom node. As the radial structure of the network has the properties of a tree, the layered based numbering scheme given in [15] has been adopted here. In this scheme, the numbering starts from top level layer where a generator terminal is treated as root node. The numbering is made for all the feeders successively in every layer as shown in Fig. 4.

C. Proposed Algorithm

1) Initialize all the elements in the microgrid network
2) Assign terminal numbers successively for all layers
3) Increment the value of step indicator k and continue if stop time has not reached
4) Assign i to the bottom most terminal
5) Compute the equivalent circuit parameters defined in (10) and (12) and accumulate its value to top terminal.
6) Decrement i and repeat step 5 until root node is reached
7) With the value of voltage at top terminal, the voltage at bottom terminal is calculated with the accumulated values of $\mathcal{Z}_i^{th}$ and $\mathcal{I}_i^k$ at feeder i
8) Increment i and repeat step 7 until the last feeder is reached
9) Repeat from step 3

D. Attack Detection Scheme

The aim of the attacker is to deceive the microgrid controller by replacing the actual values with false measurements. Since the microgrid controller acts upon the steady state values of the measurements, it is assumed in this paper that the attacker may try to manipulate those final settled values. This paper exploits the fact that due to the presence of dynamics any state change in the system will be accompanied by a unique set of transients. The proposed backward-forward sweep technique is used to calculate these transients for a given state change and later compared with the actual measurements using the following expression. The key advantage is that this BFS technique take less computation effort and hence it can be easily incorporated in light weight computing machines and obtain similar results as of the commercially available EMTP packages.

$$\Delta V = |V_{meas} - V_{calc}| \tag{14}$$

This error value ΔV is compared against a predetermined threshold to detect the presence of any data manipulation attacks. Hence for any legitimate change in system state, the values computed by the proposed BFS technique will follow the measurements. On other hand, as the transients are absent in the manipulated measurements, there will be difference between the simulated values and the obtained measurements during this transient duration. If this deviation prolongs for a extended duration then the presence of FDI attack can be concluded.

IV. Results

In order to test the performance of the proposed transient based detection scheme, a 5-bus radial microgrid given in [16] has been chosen. This test case operates in islanded mode and has 4 loads for which the power is supplied by two generators as shown in Fig. 5. Both of the generators have a rated capacity of 18.8kVA and have a terminal voltage of 400V with a rated frequency of 60 Hz. These generator ratings are considered as base values for the per unit conversion. The feeder parameters of this 5-bus radial microgrid is tabulated in Table I.

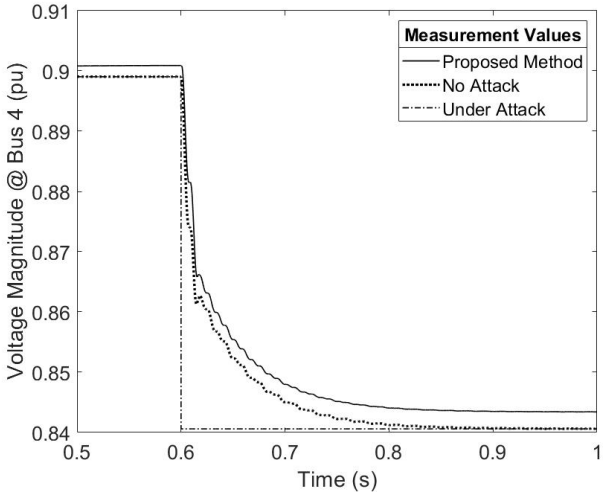


Fig. 6: Voltage magnitude measurement at Bus 4.

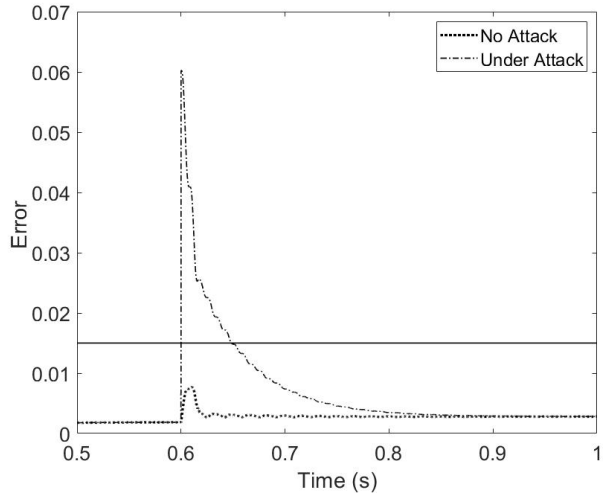


Fig. 7: Error in no attack and attack conditions.

The backward forward sweep technique for computing the electromagnetic transients has been implemented on MATAB. To obtain the measurement values, this 5-bus microgrid has be implemented in Opal-RT HYPERSIM and simulated for a period of 1 second. Bus 4 is chosen as the target bus where No-attack and attack scenarios have been considered in this implementation in HYPERSIM. The simulated values voltage magnitude at bus 4 using the proposed BFS technique and the measured values under no-attack and attack scenarios have been plotted in Fig. 6. In the no-attack scenario, the active and reactive power at bus 4 got doubled at the instant of 0.6 seconds. Due to the system dynamics, it takes a considerable period of 0.3 seconds for the voltage at bus 4 to transient from its initial value of 0.9 pu to reach the steady state value to 0.84 pu. It can be easily noticed in Fig. 6 that the proposed BFS technique provides similar results of a commercial EMTP package with less computation effort.

For the attack scenario, the aim of the attacker is to disrupt the function of the microgrid controller by falsely injecting the effect of increase in active and reactive power at bus 4 to double of its current value. In order to achieve this objective, the attacker executes a playback attack where the false steady state information has been injected at the time instant of 0.6 seconds. Replay attacks follow such attack strategy where the past values of measurements are injected such that those values may satisfy the governing equations of the microgrid under steady state condition. It is difficult for the attacker to forge a replay attack that follow the transient nature of a legitimate load change. This is because the initial conditions and the value of change in load varies time to time.

Fig. 7 shows the error between the measured values and the simulated values using the proposed BFS scheme in both no-attack and attack scenario. As both the simulated values and measured values are similar in no-attack scenario, the maximum error is around 0.0075 pu which is about less than 1%. With the detection threshold of 0.015 pu, in attack scenario, the maximum error jumps to a value around 0.06 pu and it violates the threshold only during the transient period. The threshold violation happens for a time duration of about 0.05 seconds which is more than twice the value of time period of the power supply (16.66 ms). Hence at least two threshold violations can be detected in attack scenario when the measurement devices operate at a supply frequency.

V. Conclusion and Future work

This paper presents a detection scheme for false data injection attacks against microgrid controller. This detection technique works on the principle that any change in the microgrid will be accompanied by transients due to the system dynamics and data manipulations can be detected using the mismatch in transients. To evaluate the electromagnetic transients in the radial microgrid, a backward-forward sweep based technique has been developed in this paper. The proposed BFS technique takes less computation power compared to the commercially available EMTP packages as it computes only one feeder at a given time instant. The proposed technique has been tested on a 5-bus microgrid system which is subjected to a legitimate load change and a false data injection attack that mimics such load change. It has been demonstrated that the proposed technique can able the distinguish between a legitimate load change and a false data injection attack. This work will be extended in the future by considering the detailed models of distributed energy resources such as diesel generators, battery storage system and various renewable based power generations.

References

[1] A. Hirsch, Y. Parag, and J. Guerrero, "Microgrids: A review of technologies, key drivers, and outstanding issues," *Renewable and Sustainable Energy Reviews*, vol. 90, pp. 402 – 411, 2018.

[2] D. E. Olivares, A. Mehrizi-Sani, A. H. Etemadi, C. A. Cañizares, R. Iravani, M. Kazerani, A. H. Hajimiragha, O. Gomis-Bellmunt, M. Saeedifard, R. Palma-Behnke, G. A. Jiménez-Estévez, and N. D. Hatziargyriou, "Trends in microgrid control," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1905–1919, July 2014.

[3] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 13:1–13:33, Jun. 2011.

[4] M. Rekik, Z. Chtourou, C. Gransart, and A. Atieh, "A cyber-physical threat analysis for microgrids," in *2018 15th International Multi-Conference on Systems, Signals Devices (SSD)*, March 2018, pp. 731–737.

[5] M. Chlela, G. Joos, and M. Kassouf, "Impact of cyber-attacks on islanded microgrid operation," in *Proceedings of the Workshop on Communications, Computation and Control for Resilient Smart Energy Systems*, ser. RSES '16. New York, NY, USA: ACM, 2016, pp. 1:1–1:5.

[6] S. Liu, X. Wang, and P. X. Liu, "Impact of communication delays on secondary frequency control in an islanded microgrid," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 4, pp. 2021–2031, April 2015.

[7] X. Zhang, X. Yang, J. Lin, and W. Yu, "On false data injection attacks against the dynamic microgrid partition in the smart grid," in *2015 IEEE International Conference on Communications (ICC)*, June 2015, pp. 7222–7227.

[8] M. M. Rana, Li Li, and S. W. Su, "Cyber attack protection and control in microgrids using channel code and semidefinite programming," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, July 2016, pp. 1–5.

[9] M. Chlela, G. Joos, M. Kassouf, and Y. Brissette, "Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, July 2016, pp. 1–5.

[10] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical dc microgrids," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 5, pp. 2693–2703, Oct 2017.

[11] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, "Synchrony in networked microgrids under attacks," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6731–6741, Nov 2018.

[12] A. Kondoro, I. Ben Dhaou, D. Rwegasira, A. Kelati, H. Tenhunen, and N. Mvungi, "A simulation model for the analysis of security attacks in advanced metering infrastructure," in *2018 IEEE PES/IAS PowerAfrica*, June 2018, pp. 533–538.

[13] H. Zhang, W. Meng, J. Qi, X. Wang, and W. X. Zheng, "Distributed load sharing under false data injection attack in an inverter-based microgrid," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 2, pp. 1543–1551, Feb 2019.

[14] H. W. Dommel, "Digital computer solution of electromagnetic transients in single-and multiphase networks," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-88, no. 4, pp. 388–399, April 1969.

[15] D. Shirmohammadi, H. W. Hong, A. Semlyen, and G. X. Luo, "A compensation-based power flow method for weakly meshed distribution and transmission networks," *IEEE Transactions on Power Systems*, vol. 3, no. 2, pp. 753–762, May 1988.

[16] S. Eberlein, A. Heider, and K. Rudion, "Modelling and control optimization of diesel synchronous generators in lv microgrids," in *2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, Oct 2018, pp. 1–6.