Electromagnetic Transients-Based Detection of Data Manipulation Attacks in Three Phase Radial Distribution Networks

R. James Ranjith Kumar, *Graduate Student Member, IEEE*, Biplab Sikdar, *Senior Member, IEEE*, and Deepa Kundur, *Fellow, IEEE*

***Abstract*—This article presents a detection technique for data manipulation attacks in distribution systems using transient information present in the measurements. This technique is based on the fact that any legitimate changes in the system will have a transient response which can be measured by the monitoring system. An algorithm is developed for obtaining the transient solution for three-phase distribution networks. A backward–forward sweep technique is developed for the proposed radial electromagnetic transient program (EMTP) which exploits the radial structure of distribution network. An inclusive transient model compatible with the proposed three-phase radial EMTP for three-phase synchronous generators is also developed. The proposed radial EMTP has been benchmarked with conventional EMTP with 5-bus and 22-bus radial distribution systems and with the same test systems, the proposed detection functionality is evaluated. It is shown that the transient solution provided by radial EMTP are in agreement with the results of conventional EMTP. It is also demonstrated that the deviations between the measured values and the solution of the radial EMTP increase significantly during the transient period when a data manipulation attack is carried out.**

***Index Terms*—Distribution system, electromagnetic transient program (EMTP), stealthy attack, synchronous generator, transients.**

I. Introduction

DISTRIBUTION systems are as vulnerable as transmission systems to cyberattacks since both use a similar SCADA architecture for their monitoring and control operations. Data manipulation attacks are a class of cyberattacks which aim to mislead the central controller [which can be a distribution management system (DMS) or microgrid controller] by injecting false values in place of the actual measurements that are collected in the network. Such (appropriately designed) data manipulation attacks can bypass conventional bad data detection schemes since the manipulated values comply with the steady-state model of the network [1]. Due to the smaller size of distribution systems (as compared to transmission systems), the data manipulation attacks not just manipulate a subset of measurements [2], but the whole available set of measurements available in the distribution network. This data manipulation results in convincing the monitoring system that a state change has happened in the distribution system even though it does not correspond to the ground reality [3]. A false alteration in the system state (e.g., creating a fake load change) could trigger the central controller to take an unnecessary control action (like adjusting its local generation and power fed by the grid) which can destabilize the power balance in the system and lead to devastating consequences. Legitimate state changes can happen due to changes in loads or changes in network topology. Load levels change more frequently in a distribution network as compared to topology changes. Hence, a fake load change injected through data manipulation attacks can be concealed along with the natural changes in load. In contrast, a fake topology change has a high likelihood of triggering suspicion in the eyes of the system operator [4].

To address the security concerns highlighted above, this article develops a technique for detecting fake load changes caused due to data manipulation attacks in distribution systems. The proposed technique validates that any reported state change has happened only due to a corresponding change in the load and hence, it can distinguish a fake load change from a legitimate one. The proposed detection technique is based on the fact that any state change is accompanied by a set of transients due to the presence of dynamic circuit elements in the system. In order to implement the detection mechanism, this article develops a radial EMTP algorithm which obtains the transient solution of a radial distribution network and later compares them against the available measurements in the network to identify the presence of data manipulation attacks. EMTP is one of the common methods used in power systems and power electronics to obtain a transient solution [5]. While different versions of EMTPs have been introduced over the last four decades, all such versions use nodal analysis variants to obtain the transient solution [6].

Manuscript received January 31, 2021; revised August 16, 2021; accepted September 15, 2021. Date of publication November 12, 2021; date of current version January 14, 2022. This work was supported by the Singapore Ministry of Education Academic Research Fund Tier 1 under Grant R-263-000-D01-114. Paper 2020-SECSC-1805.R1, presented at the 2020 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES), Jaipur, India, Dec. 16–19, and approved for publication in the IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS by the Renewable and Sustainable Energy Conversion Systems Committee of the IEEE Industry Applications Society. *(Corresponding author: Biplab Sikdar.)*

R. James Ranjith Kumar and Biplab Sikdar are with the National University of Singapore, Singapore 119077, Singapore (e-mail: jamesranjithkumar@u.nus.edu; bsikdar@nus.edu.sg).

Deepa Kundur is with the University of Toronto, Toronto, ON M5S 1A1, Canada (e-mail: dkundur@ece.utoronto.ca).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIA.2021.3127859.

Digital Object Identifier 10.1109/TIA.2021.3127859

The reason for such a wide adoption of nodal analysis is with the consideration that the networks usually have meshed form. With nodal analysis, EMTP is required to solve linear equations simultaneously for each time step. This article develops an efficient algorithm for obtaining the transient solution and exploits the radial nature of the distribution network. The proposed method also develops a model for synchronous generators where no predictions or corrections are required for any of its variables and it can be included the radial EMTP in a simple manner.

The remainder of this article is organized as follows. Section II presents an overview of the related work and the attack model. Section III presents the detection methodology for data manipulation attacks on distribution networks. It also develops the necessary mathematical formulations and the backward-forward sweep methodology to obtain the transient solution of three phase radial networks. In Section IV, a technique is proposed to interface the three phase synchronous generator model with the developed radial EMTP algorithm. The proposed radial EMTP algorithm and the data manipulation detection technique are validated in Section V. Finally, Section VI concludes this article.

II. Data Manipulation Attacks

A. Related Work

A general overview of the cybersecurity aspects of distribution systems is explored in [7]. An attack strategy is developed in [8] whose objective is to manipulate the status of overcurrent relay and circuit breaker in a distribution feeder. Stealthy attacks that can circumvent traditional bad data detection schemes in distribution systems are developed in [9] that generate the attack vector using an approximate estimate of state. Such stealthy attacks are studied in [10] that target linear polyphase distribution system state estimators. Access points for cyberattacks on microgrids include the terminals of distributed generations, the medium of communication, or at the controller itself [11]. It is shown in [12] that by creating delay in the communication channel between the measurement samples may have a major impact on the operation of the distribution network. It is demonstrated in [13] that false data injection (FDI) attacks on the distribution networks can have significant impact on the values of active power flow and system frequency.

The vulnerabilities in a microgrid and possible threats are mentioned in [14]. It is demonstrated in [15] that the process of islanding can be disrupted with FDI attacks. With consideration the AMI infrastructure, an attack model is developed in [16] to execute FDI attacks on microgrids. A comprehensive study on the impact of FDI attacks on inverter-based microgrid is conducted in [17].

While the vulnerabilities of distribution systems and the challenges they pose, there is a lack of effective methods to detect them. This article addresses this open problem and proposed a physical-law based detection methodology.

B. Attack Model

In a typical SCADA system used for distribution networks, load levels are monitored using the values of bus power injections which are measured using remote terminal units (RTU). In order to describe the attack model, let $\mathring{\mathcal{S}}^k$ be the vector of complex power injections measured at all buses corresponding to the kth time instant. With this definition, the power balance equation can be written as

$$\mathring{\mathcal{S}}^k = \mathring{\mathcal{V}}^k \odot \left(\mathring{\mathcal{I}}^k\right)^* \tag{1}$$

where $\mathring{\mathcal{V}}^k$ and $\mathring{\mathcal{I}}^k$ are the vectors of complex voltage and current phasors at all buses corresponding to the kth time instant, respectively. The notations $\odot$ and $(\cdot)^*$ indicate the element wise multiplication and complex conjugate, respectively.

Due to the smaller geographical size of the distribution system, the attacker can manipulate all available measurements present in the targeted network. However, due to the stochastic nature of the loads, the attacker cannot obtain the exact load information at the instant of the attack. To deceive the central controller with a load change $\Delta\mathcal{S}$, the manipulated complex power measurements that can replace the actual measurements is written as

$$\dot{\mathcal{S}}^k = \mathring{\mathcal{S}}^k + \Delta\mathcal{S} \tag{2}$$

where

$$\Delta\mathcal{S} = \Delta\mathcal{V} \odot (\Delta\mathcal{I})^* + \mathring{\mathcal{V}}^k \odot (\Delta\mathcal{I})^* + \Delta\mathcal{V} \odot \left(\mathring{\mathcal{I}}^k\right)^*. \tag{3}$$

To execute such a load manipulation attack, it is assumed that the attacker is able to get the complete network information from which the line parameters can be extracted. With the network information, the attacker can calculate the complex valued bus impedance matrix of the targeted distribution network. In order to calculate the amount of voltage change in all the bus measurements for a fake load change, it is considered that $\Delta\mathcal{I}$ is the vector of change in current injection in all buses corresponding to the fake load change intended by the attacker. Let $\mathcal{Z}$ be the complex valued bus impedance matrix of the distribution network which is also available to the attacker. Then, the required voltage change to be made in all the buses to fake a load change can be written as

$$\Delta\mathcal{V} = \mathcal{Z}\Delta\mathcal{I}. \tag{4}$$

The voltage magnitudes in distribution networks are usually regulated to a value closer to the grid voltage. Also, the amount of fake load change intended by the attacker is a function of the change in bus voltages and current injections. Hence, (3) can be written as $\Delta\mathcal{S} = f(\Delta\mathcal{V}, \Delta\mathcal{I})$ where $\Delta\mathcal{V}$ and $\Delta\mathcal{I}$ are related as shown in (4). Note that with this consideration, the attacker does not require the current load information even though it requires all the measurement values in the network to be manipulated to fake a load change. Also, with the principle of superposition, it is easy to see that any legitimate load changes in any of the buses will not affect the solution of this data manipulation process. This process of data manipulation can be extended from the instant of attack initiation unto the point desired by the attacker to fake the voltage. Thus, by selecting the value of $\Delta\mathcal{I}$, the attacker can obtain $\Delta\mathcal{V}$ and can manipulate the measured values to $\dot{\mathcal{S}}^k$ from its original value of $\mathring{\mathcal{S}}^k$. With such manipulated measurements,

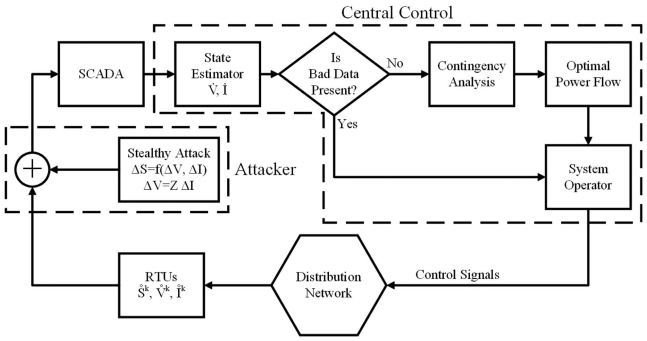

Fig. 1. Illustration of the load falsification attack scheme.

the state estimator output can be manipulated to $\dot{\mathcal{V}}^k$ and $\dot{\mathcal{I}}^k$ from its actual value of $\mathring{\mathcal{V}}^k$ and $\mathring{\mathcal{I}}^k$ as

$$\dot{\mathcal{V}}^k = \mathring{\mathcal{V}}^k + \Delta\mathcal{V} \tag{5}$$

$$\dot{\mathcal{I}}^k = \mathring{\mathcal{I}}^k + \Delta\mathcal{I}. \tag{6}$$

Such a load falsification attack is illustrated in Fig. 1. Conventional bad data detection schemes check for the compliance of state estimator outputs with the steady-state system model. Since the amount of manipulations $\Delta\mathcal{S}$, $\Delta\mathcal{V}$, and $\Delta\mathcal{I}$ satisfy the power balance equations of the given distribution network, this attack scheme cannot be detected with conventional bad data schemes. Hence, such manipulated state values could make the system operator to take incorrect control actions based on the fake load change which may affect the stable operation of the distribution network. In the next section, we propose a detection scheme which uses the transient components present in the measurements to detect the presence of stealthy load falsification attacks.

III. Proposed EMTP for Radial Networks

A. Principle of Proposed Detection Technique

To detect the presence of data manipulation attacks, the proposed detection technique checks whether the transient components present in the measured values are in agreement with the system dynamics of the given distribution network. To develop such a technique, consider that a significant load change is identified at time instant k_0. It is considered that $\widehat{\mathcal{V}}^k$ is the vector of voltage magnitude measurements of all the available buses at time instants $k \in \{k_0, k_0+1, k_0+2, \ldots, k_0+w\}$. The size of measurement window w is selected depending upon the time up to which the transient components persist for the given distribution system.

The purpose of the proposed detection technique is to detect whether the measurements $\widehat{\mathcal{V}}^k$, $\forall\, k \in \{k_0, k_0+1, k_0+2, \ldots, k_0+w\}$ are either manipulated, $\dot{\mathcal{V}}^k$, or legitimate, $\mathring{\mathcal{V}}^k$. To carry out this detection process, the transient solution is obtained with the available information of the load change for the time period between k_0 to k_0+w. Let $\widetilde{\mathcal{V}}^k$ for $k \in \{k_0, k_0+1, k_0+2, \ldots, k_0+w\}$ be the transient solution obtained through simulation. Hence, for any legitimate load change in the system, the computed values $\widetilde{\mathcal{V}}^k$ will follow the measurements $\widehat{\mathcal{V}}^k$, $\forall k \in [k_0, k_0+w]$. Whereas in the manipulated measurements, the transients components will be absent and hence the simulated values, $\widetilde{\mathcal{V}}^k$ will not be in agreement the obtained measurements, $\widehat{\mathcal{V}}^k$, during this transient period. If these variations are present over a longer period of time, the existence of a data manipulation attack can be inferred. With this principle, a procedure is developed for detecting data manipulation attacks and given in Algorithm 1.

Algorithm 1: Data Manipulation Attack Detection Technique.

for every incoming measurement **do**
  Calculate the amount of load change in all buses
  if any significant load change is identified **then**
    $C \Leftarrow 0$
    Identify location and k_0 where load change happened
    Obtain the transient solution $\widetilde{\mathcal{V}}^k\ \forall k \in [k_0, k_0+w]$
    for $k = k_0$ to k_0+w **do**
      $\Delta\mathcal{E}^k \Leftarrow |\widetilde{\mathcal{V}}^k - \widehat{\mathcal{V}}^k|$
      if $\Delta\mathcal{E}^k \geq \tau$ **then**
        $C \Leftarrow C+1$
      end if
    end for
    if $C \geq \eta$ **then**
      print "System is under attack"
    end if
  end if
end for

In Algorithm 1, $\Delta\mathcal{E}^k$ is the error value between the calculated values $\widetilde{\mathcal{V}}^k$, and the measurements $\widehat{\mathcal{V}}^k$, at time instant k. The variable C counts the number of instances when $\Delta\mathcal{E}^k$ violates the threshold τ. If there are more than η threshold violations, it can be inferred that the transient components in the measured values are not in agreement with the system dynamics and the measurements are considered to be manipulated. As the detection process in the proposed technique depends entirely upon the methodology for obtaining the transient solution, a radial EMTP technique that takes less computation effort is developed in the next section.

B. Modeling of Network

EMTP handles the dynamic circuit elements by converting them into interconnections of resistive values with current or voltage sources that carries forward the information of the previous time steps. This rationale is illustrated in Table I which shows that to obtain the transient solution at a given time step, EMTP requires to solve a linear dc network built using these discrete models and conventional EMTP solves such a dc

TABLE I
DESCRIPTION OF EMTP MODELS FOR BASIC ELEMENTS

Resistor	$i^k_{m,n} = \dfrac{1}{R}\left(v^k_m - v^k_n\right)$
Inductor	$i^k_{m,n} = \dfrac{\Delta t}{2L}\left(v^k_m - v^k_n\right) + H^{k-1}_L$ $H^k_L = \dfrac{\Delta t}{L}\left(v^k_m - v^k_n\right) + H^{k-1}_L$
Capacitor	$i^k_{m,n} = \dfrac{2C}{\Delta t}\left(v^k_m - v^k_n - H^{k-1}_C\right)$ $H^k_C = 2(v^k_m - v^k_n) - H^{k-1}_C$

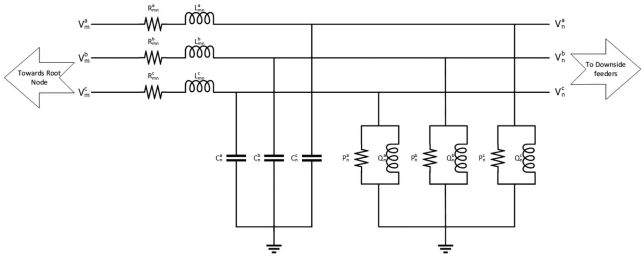

Fig. 2. Line section.

network using nodal analysis. In contrast, the proposed method follows a branch oriented approach to exploit the radial structure of distribution networks. For each time step, the proposed technique follows a two stage computation process, namely, backward sweep and forward sweep.

To develop the radial EMTP technique using backward–forward sweep (BFS) algorithm, consider a three phase line section in a radial network between buses m and n as shown in Fig. 2 where bus m is closer to the root node as compared to bus n. Hence, bus m is denoted as upside bus and bus n as downside bus. Let the three-phase branch elements given in Fig. 2 be represented in matrix form as $\bar{\mathbf{R}}_{mn}$, $\bar{\mathbf{L}}_{mn}$, and $\bar{\mathbf{C}}_n$. The resistive and inductive values of the load at bus n are denoted as $\bar{\mathbf{P}}_n$ and $\bar{\mathbf{Q}}_n$, respectively. Similarly, the history components of corresponding elements are denoted in vector form as $\bar{\mathbf{H}}^{k-1}$ whose subscripts denote its associated element. With these notations, the cumulative formulations utilized in backward and froward sweeps are developed as follows.

1) Backward Sweep: As the name indicates, backward sweep starts the cumulative computation from the terminal nodes (nodes other than the root node at which only one branch is incident) and proceeds toward the root node. The aim of the backward sweep is to compute the values of equivalent conductance and equivalent current for each of the buses looking back toward the downside feeders in the network. To develop the cumulative update rule for the backward sweep, it is considered that the backward sweep is conducted up to bus n where the equivalent conductance and equivalent current looking back toward all the downside feeders from bus n are calculated as $\bar{\mathbf{Y}}_n$ and $\bar{\mathbf{H}}^{k-1}_{\bar{\mathbf{Z}}_n}$, respectively. These definitions can be used to build the discretized equivalent of the line section between buses m and n as shown in Fig. 3. To simply the formulation, the shunt values corresponding to elements $\bar{\mathbf{C}}_n$, $\bar{\mathbf{P}}_n$, $\bar{\mathbf{Q}}$, and $\bar{\mathbf{Y}}_n$ can be

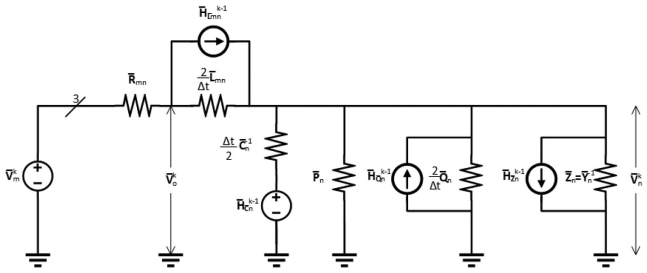

Fig. 3. EMTP model equivalent.

combined together as

$$\bar{\mathcal{R}}_n = \left(\frac{2}{\Delta t}\bar{\mathbf{C}}_n + \bar{\mathbf{P}}^{-1}_n + \frac{\Delta t}{2}\bar{\mathbf{Q}}^{-1}_n + \bar{\mathbf{Y}}_n\right)^{-1}. \tag{7}$$

Similarly, the components $\bar{\mathbf{H}}^{k-1}_{\bar{\mathbf{C}}_n}$, $\bar{\mathbf{H}}^{k-1}_{\bar{\mathbf{Q}}_n}$, and $\bar{\mathbf{H}}^{k-1}_{\bar{\mathbf{Z}}_n}$ can be merged as

$$\bar{\mathcal{J}}^{k-1}_n = \frac{2}{\Delta t}\bar{\mathbf{C}}_n\bar{\mathbf{H}}^{k-1}_{\bar{\mathbf{C}}_n} - \bar{\mathbf{H}}^{k-1}_{\bar{\mathbf{Q}}_n} + \bar{\mathbf{H}}^{k-1}_{\bar{\mathbf{Z}}_n}. \tag{8}$$

With this consideration, the cumulative update rule for looking back conductance from bus m can be written as

$$\bar{\mathbf{Y}}_m \Leftarrow \bar{\mathbf{Y}}_m + \bar{\mathbf{Z}}^{-1}_m \tag{9}$$

where

$$\bar{\mathbf{Z}}_m = \bar{\mathbf{R}}_{mn} + \frac{2}{\Delta t}\bar{\mathbf{L}}_{mn} + \bar{\mathcal{R}}_n. \tag{10}$$

By using the principle of superposition and current division rule, the cumulative update rule for the value of drawn equivalent current seen from bus m can be expressed as

$$\bar{\mathbf{H}}^{k-1}_{\bar{\mathbf{Z}}_m} \Leftarrow \bar{\mathbf{H}}^{k-1}_{\bar{\mathbf{Z}}_m} + \bar{\mathbf{Z}}^{-1}_m\left(\bar{\mathcal{R}}_n\bar{\mathcal{J}}^{k-1}_n - \frac{2}{\Delta t}\bar{\mathbf{L}}_{mn}\bar{\mathbf{H}}^{k-1}_{\bar{\mathbf{L}}_{mn}}\right). \tag{11}$$

For the kth time step, the values of $\bar{\mathbf{Y}}_m$ and $\bar{\mathbf{H}}^{k-1}_{\bar{\mathbf{Z}}_m}$ are initialized as zero at the start of the backward sweep for all the buses. By using the update rules given in (9) and (11), at the end of the backward sweep, equivalent conductance and the equivalent current drawn for all the buses can be calculated.

2) Forward Sweep: The forward sweep is initiated after the backward sweep is completed for the given time step. In this sweep, the instantaneous values of bus voltages and branch currents at the given time step are calculated using the values of looking back conductance and the equivalent current drawn for each bus which are computed during the backward sweep. On contrast to the backward sweep, the forward sweep starts from the root node and traverses downward toward the terminal nodes. To develop the formulations for this forward sweep process, it is considered that the forward sweep is executed up to bus m and hence its instantaneous voltage value, $\bar{\mathbf{v}}^k_m$ at the kth time step is available. With this value along with $\bar{\mathbf{Y}}_m$ and $\bar{\mathbf{H}}^{k-1}_{\bar{\mathbf{Z}}_m}$ which are computed during the backward sweep, the nodal voltages $\bar{\mathbf{v}}^k_o$ and $\bar{\mathbf{v}}^k_n$ corresponding to the line section between m and n can be given as

$$\begin{bmatrix}\bar{\mathbf{v}}^k_o \\ \bar{\mathbf{v}}^k_n\end{bmatrix} = \bar{\mathcal{Y}}^{-1}_{mn}\bar{i}^{k-1}_{mn} \tag{12}$$

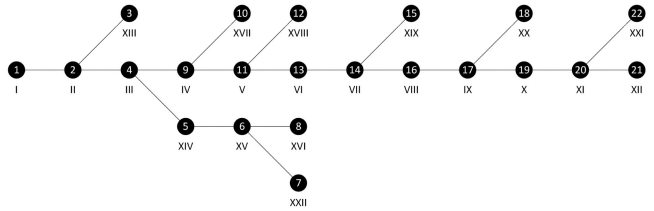

Fig. 4. Illustration of the proposed sequence ordering scheme.

where

$$\bar{\mathcal{Y}}_{mn} = \begin{bmatrix} \bar{\mathbf{R}}_{mn}^{-1} + \frac{\Delta t}{2}\bar{\mathbf{L}}_{mn}^{-1} & -\frac{\Delta t}{2}\bar{\mathbf{L}}_{mn}^{-1} \\ -\frac{\Delta t}{2}\bar{\mathbf{L}}_{mn}^{-1} & \bar{\mathcal{R}}_{n}^{-1} + \frac{\Delta t}{2}\bar{\mathbf{L}}_{mn}^{-1} \end{bmatrix} \tag{13}$$

$$\bar{i}_{mn}^{k-1} = \begin{bmatrix} \bar{\mathbf{R}}_{mn}^{-1}\bar{\mathbf{v}}_{m}^{k} - \bar{\mathbf{H}}_{\bar{\mathbf{L}}_{mn}}^{k-1} \\ \bar{\mathcal{J}}_{n}^{k-1} + \bar{\mathbf{H}}_{\bar{\mathbf{L}}_{mn}}^{k-1} \end{bmatrix}. \tag{14}$$

With $\bar{\mathbf{v}}_o^k$ and $\bar{\mathbf{v}}_n^k$, the branch current $\bar{\mathbf{i}}_{m,n}^k$ flowing through the line section between m and n can be calculated as

$$\bar{\mathbf{i}}_{m,n}^{k} = \bar{\mathbf{R}}_{mn}^{-1}\left(\bar{\mathbf{v}}_{m}^{k} - \bar{\mathbf{v}}_{o}^{k}\right). \tag{15}$$

It is noticed that instead of carrying out the nodal analysis for the entire network for each time step (which is the case with conventional EMTP), the proposed radial EMTP solved each of the line sections in a sequential manner which reduces the computational effort. In addition to calculating the bus voltages and branch currents, the forward sweep updates the history terms corresponding to the dynamic circuit elements of each line section. The update rule for the history terms of $\overline{\mathbf{L}}_{mn}$, $\overline{\mathbf{C}}_n$, and $\overline{\mathbf{Q}}_n$ for a given line section between m and n is easily derived from the models given in Table I which can be written as

$$\bar{\mathbf{H}}_{\bar{\mathbf{L}}_{mn}}^{k} = \Delta t\, \bar{\mathbf{L}}_{mn}^{-1}\left(\bar{\mathbf{v}}_{o}^{k} - \bar{\mathbf{v}}_{n}^{k}\right) + \bar{\mathbf{H}}_{\bar{\mathbf{L}}_{mn}}^{k-1} \tag{16}$$

$$\bar{\mathbf{H}}_{\bar{\mathbf{C}}_n}^{k} = 2\bar{\mathbf{v}}_{n}^{k} - \bar{\mathbf{H}}_{\bar{\mathbf{C}}_n}^{k-1} \tag{17}$$

$$\bar{\mathbf{H}}_{\bar{\mathbf{Q}}_n}^{k} = \Delta t\, \bar{\mathbf{Q}}_{n}^{-1}\bar{\mathbf{v}}_{n}^{k} + \bar{\mathbf{H}}_{\bar{\mathbf{Q}}_n}^{k-1}. \tag{18}$$

C. Bus Sequence Ordering Scheme

To execute the BFS technique, the sequence of buses and its corresponding branches have to be ordered such that the looking back conductance and the equivalent current toward the downside bus are available to compute the equivalents from the upside bus. Such an ordering sequence is also needed in the forward sweep where the upside bus voltage should be available before calculating the downside bus voltage.

The proposed bus sequence ordering scheme is shown in Algorithm 2. This algorithm requires a search program, a bookkeeping register, a stack, and a queue. The bookkeeping register marks the index value of the branches which are entered in either stack or queue. The search program finds the list of branches that are not listed in the bookkeeping register and connected to the selected node. The elements of the stack follow last in first out order and it consists of two operations, namely, push and pop. On the contrary, the elements of the queue follows first in first out order and it consists of two operations, namely, enqueue and dequeue. The enqueue operation of a queue adds the given element in the rear most position of the queue whereas the dequeue operation returns the entry at the front most position of the queue.

Algorithm 2: Bus Sequence Ordering Scheme.

```
Assign root node as selected bus
Initialize selected bus with first sequence number
repeat
    Search for non-visited branches linked to selected bus
    if search results are empty
        Dequeue a branch number & push it in Stack
    else
        Mark branches in search results as visited
        Push one of the search result in Stack
        Enqueue the remaining search results in Queue
    end if
    Assign downside bus of popped branch as selected bus
    Assign consequent sequence number to selected bus
until sequence number assigned to all buses
```

This bus sequence ordering scheme is illustrated in Fig. 4 using the 22-bus radial distribution topology given in [18]. The bus numbers are indicated on the nodes in Arabic numerals and their corresponding sequence numbers are denoted in Roman numerals below each node.

D. Radial EMTP Algorithm

Using the network models and the ordering scheme developed in the earlier part of this section, the radial EMTP that follows the BFS technique is shown in Algorithm 3. The ordering sequence obtained for the buses can be easily extended to the branches as the index of a downside bus can be interchangeably used with its corresponding branch. With this technique, a single line section is solved for a given time step rather than solving the entire network for each time step which is in the case of conventional EMTP. Switching elements like circuit breakers are modeled as variable resistance in a similar manner as it is done in conventional EMTP where the resistance value is negligible during closed state and it can be increased to an extremely high value to simulate the open state. As the elements in the distribution systems can be modeled using the lumped values of resistance, inductance and capacitance, they can be easily integrated in the proposed radial EMTP algorithm using their equivalent circuit. In the next section, we use such an approach to interface the synchronous machine model with the radial EMTP.

It can be noticed that in the proposed radial EMTP, the formulations are made in recursive form using the bus sequence ordering scheme which exploits the radial nature of distribution systems. This recursive formulation is similar to a triangular linear system and solved using the BFS technique. The BFS technique is identical to the forward and backward substitution method for solving a triangular system of linear simultaneous equations and hence it has arithmetic complexity of $\mathcal{O}(n^2)$ [19].

Algorithm 3: Radial EMTP Using the BFS Technique.

Assign step time, Δt according to the given problem
Assign sequence numbers to all branches
repeat
  Update positions of switching elements and loads
  Update the equivalent circuit of generations
  for lines $\{m, n\}$ from last sequence number to first **do**
    Calculate $\bar{\mathbf{Y}}_m$ and $\bar{\mathbf{H}}_{\bar{\mathbf{Z}}_m}^{k-1}$ using (9) and (11)
  end for
  Calculate instantaneous voltage value at root node for this time instant
  for lines $\{m, n\}$ from first sequence number to last **do**
    Calculate $\bar{\mathbf{v}}_o^k$, $\bar{\mathbf{v}}_n^k$ and $\bar{\mathbf{i}}_{m,n}^k$ using (12) and (15)
    Update history terms using (16), (17) and (18)
  end for
  Update terms for generations
  Increment the time step index, k
until stop time is reached

On the other hand, conventional EMTP uses nodal analysis, and Gaussian elimination-based techniques are popularly used to solve its linear system which has computational complexity of $\mathcal{O}(n^3)$ [20]. This is because conventional EMTPs are built to accommodate any type of electrical topology and they are not able to exploit the radial structure of the distribution networks. As the proposed radial EMTP approach takes lesser computational effort as compared to conventional EMTP for radial distribution networks, radial EMTP can provide the transient solution faster than the conventional EMTP techniques. Hence, this technique can detect the presence of data manipulation attacks more quickly as compared to the conventional EMTPs.

IV. Synchronous Machine Model

Existing EMTP models for synchronous machines [21] can be classified as classical *dq*0 model, phase domain model, and voltage behind reactance model. One issue in all such models is that at least two of the variables need to be predicted before solving the corresponding machine at each time step and then, these predicted values need to be corrected (e.g., in the classical *dq*0 model, prediction and correction of speed voltages in *d*- and *q*-axes are carried out for every time step [22]). Such prediction and correction processes not only take significant computation power but also can reduce the simulation accuracy and numerical stability.

Since a synchronous machine is an electro-mechanical device, to obtain its transient response, modeling is carried out for the mechanical part and the electrical part. The mechanical part is traditionally modeled using the swing equation and that can be easily solved to obtain the angular velocity ω_r and the rotor position θ can be calculated. On the other hand, modeling the electrical part of a three phase synchronous machine is quite challenging as the values of coupled and self inductance in the armature, field, and damper windings vary with respect to θ.

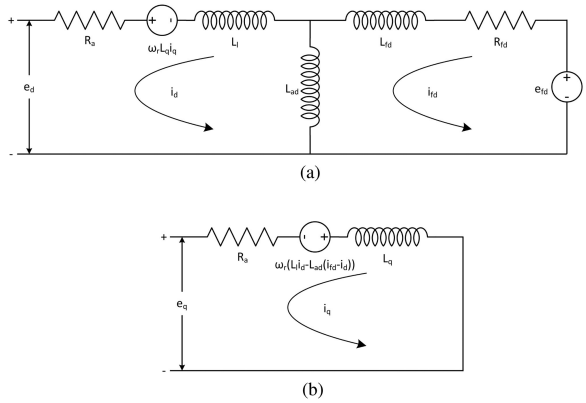

Fig. 5. Synchronous generator equivalent circuit. (a) Direct axis. (b) Quadrature axis.

Classically, this issue can be resolved using Park's transformation where the machine variables corresponding to phase domain are transformed for the direct and quadrature magnetic rotor axes. As a result, the time varying inductances in the three phase armature, field and damper windings can be converted as fixed values in a single rotating reference frame. Let i_a, i_b, and i_c be the armature phase currents of the synchronous generator. With Park's transformation, the projections of these phase currents in direct and quadrature axes can be written as

$$\begin{bmatrix} i_d & i_q \end{bmatrix}^T = \mathbf{K}_{\mathcal{P}} \begin{bmatrix} i_a & i_b & i_c \end{bmatrix}^T \tag{19}$$

where

$$\mathbf{K}_{\mathcal{P}} = \frac{2}{3}\begin{bmatrix} \cos(\theta) & \cos\left(\theta - \frac{2\pi}{3}\right) & \cos\left(\theta + \frac{2\pi}{3}\right) \\ -\sin(\theta) & -\sin\left(\theta - \frac{2\pi}{3}\right) & -\sin\left(\theta + \frac{2\pi}{3}\right) \end{bmatrix}. \tag{20}$$

For the purpose of illustration, Model 1.0 of a three phase synchronous machine [23] is considered whose elemental notations are adopted from [24]. Such a model is considered as the values of damper winding resistances is relatively high in small and medium sized synchronous generators and due to that, its damper windings do not provide much contribution to the magnetic fields present in the *d*- and *q*-axes during the operating conditions. Hence, by neglecting the parameters and equations related to the damper windings, the complexity and the size of the model is reduced without losing much of the accuracy [25]. The governing equations of the electrical part for such a synchronous generator can be written as

$$e_d = -R_a i_d - (L_{ad} + L_l)\frac{d}{dt} i_d + L_{ad}\frac{d}{dt} i_{fd} + \omega_r L_q i_q \tag{21}$$

$$e_q = -R_a i_q - L_q \frac{d}{dt} i_q - \omega_r (L_l i_d - L_{ad}(i_{fd} - i_d)) \tag{22}$$

$$e_{fd} = R_{fd} i_{fd} + (L_{fd} + L_{ad})\frac{d}{dt} i_{fd} - L_{ad}\frac{d}{dt} i_d. \tag{23}$$

With these governing equations, the equivalent circuit in direct and quadrature axes can be developed for a Model 1.0 three phase synchronous machine as shown in Fig. 5. Hence, the process of obtaining the transient solution of such synchronous machine comes down to solving a circuit with the elements of resistance, inductance, and current controlled voltage sources.

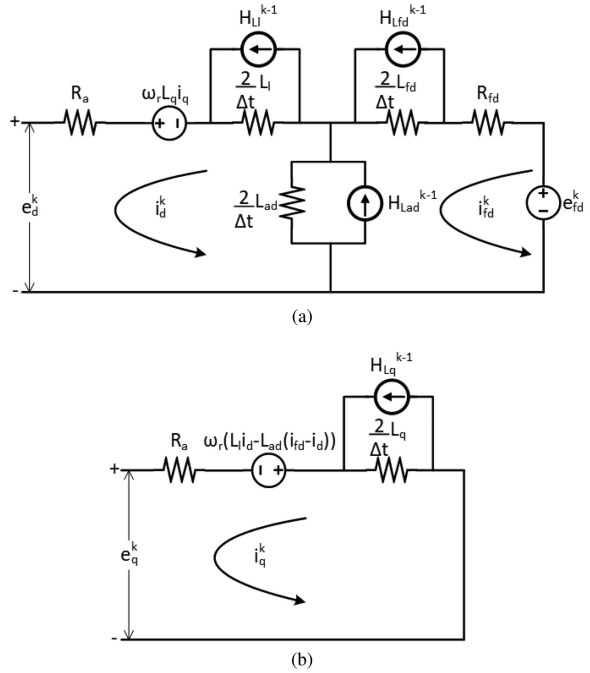

Fig. 6. EMTP model for synchronous generator. (a) Direct axis. (b) Quadrature axis.

To convert the differential equations into algebraic form, the inductive elements in this equivalent circuit are replaced with their discrete EMTP models as illustrated in Fig. 6. Let $H_{L_l}^{k-1}$, $H_{L_{ad}}^{k-1}$, $H_{L_{fd}}^{k-1}$, and $H_{L_q}^{k-1}$ be the history terms at $k-1$ time step corresponding to elements L_l, L_{ad}, L_{fd}, and L_q, respectively. As the field voltage is supplied by an external source, without loss of generality, the values of e_{fd}^k are considered to be known for every time step k. With this consideration and by simple algebraic manipulations, the relation between the voltages e_d^k, e_q^k and the currents i_d^k, i_q^k for the time step k can be written as

$$\begin{bmatrix} e_d^k \\ e_q^k \end{bmatrix} = \begin{bmatrix} \mathcal{V}_d^{k-1} \\ \mathcal{V}_q^{k-1} \end{bmatrix} - \begin{bmatrix} \mathcal{Z}_{dd}^k & \mathcal{Z}_{dq}^k \\ \mathcal{Z}_{qd}^k & \mathcal{Z}_{qq}^k \end{bmatrix} \begin{bmatrix} i_d^k \\ i_q^k \end{bmatrix} \tag{24}$$

where

$$\mathcal{Z}_{dd}^k = R_a + \frac{2}{\Delta t} L_l + \left(\frac{1}{R_{fd} + \frac{2}{\Delta t} L_{fd}} + \frac{1}{\frac{2}{\Delta t} L_{ad}} \right)^{-1} \tag{25}$$

$$\mathcal{Z}_{qq}^k = R_a + \frac{2}{\Delta t} L_q \tag{26}$$

$$\mathcal{Z}_{dq}^k = -\omega_r^k L_q \tag{27}$$

$$\mathcal{Z}_{qd}^k = \omega_r^k \left(L_l + L_{ad} - \frac{L_{ad}^2}{\frac{\Delta t}{2} R_{fd} + L_{fd} + L_{ad}} \right) \tag{28}$$

and

$$\mathcal{V}_d^{k-1} = \frac{\left(\frac{e_{fd}^k + \frac{2}{\Delta t} H_{L_{fd}}^{k-1} L_{fd}}{R_{fd} + \frac{2}{\Delta t} L_{fd}} + H_{L_{ad}}^{k-1} \right)}{\left(\frac{1}{R_{fd} + \frac{2}{\Delta t} L_{fd}} + \frac{1}{\frac{2}{\Delta t} L_{ad}} \right)} \tag{29}$$

$$\mathcal{V}_q^{k-1} = \omega_r L_{ad} \left(\frac{e_{fd}^k + \frac{2}{\Delta t} \left(H_{L_{fd}}^{k-1} L_{fd} - H_{L_{ad}}^{k-1} L_{ad} \right)}{R_{fd} + \frac{2}{\Delta t} \left(L_{fd} + L_{ad} \right)} \right) + \frac{2}{\Delta t} H_{L_q}^{k-1} L_q. \tag{30}$$

The model given in (24) can be represented as a two port equivalent circuit with $\mathcal{Z}_{dd}^k$, $\mathcal{Z}_{dq}^k$, $\mathcal{Z}_{qd}^k$, and $\mathcal{Z}_{qq}^k$ as the elements of equivalent resistance matrix and the values of open circuit voltage are given by $\mathcal{V}_d^{k-1}$ and $\mathcal{V}_q^{k-1}$. Such a model can be used to interface multiple synchronous machines in the backward and forward sweeps of the proposed radial EMTP. To demonstrate the proposed interfacing technique in the radial EMTP, consider a synchronous machine that is connected to bus n in the given radial network. Prior to starting the backward sweep for the time step k, the looking back conductance corresponding to bus n is updated using the the elements of Thevenin's resistance matrix to its respective synchronous machine as

$$\bar{\mathbf{Y}}_n \Leftarrow \bar{\mathbf{Y}}_n + \frac{3}{2} \mathbf{K}_{\mathscr{P}}^T \begin{bmatrix} \mathcal{Z}_{dd}^k & \mathcal{Z}_{dq}^k \\ \mathcal{Z}_{qd}^k & \mathcal{Z}_{qq}^k \end{bmatrix}^{-1} \mathbf{K}_{\mathscr{P}}. \tag{31}$$

Similarly, the equivalent current value at bus n can be updated using the values of open circuit voltage of its respective synchronous machine as

$$\bar{\mathbf{H}}_{\bar{\mathbf{Z}}_n}^{k-1} \Leftarrow \bar{\mathbf{H}}_{\bar{\mathbf{Z}}_n}^{k-1} + 3\mathbf{K}_{\mathscr{P}}^T \begin{bmatrix} \mathcal{Z}_{dd}^k & \mathcal{Z}_{dq}^k \\ \mathcal{Z}_{qd}^k & \mathcal{Z}_{qq}^k \end{bmatrix}^{-1} \begin{bmatrix} \mathcal{V}_d^{k-1} \\ \mathcal{V}_q^{k-1} \end{bmatrix}. \tag{32}$$

After completing the forward sweep for time step k, the instantaneous voltage value at time step k is available for all the buses. With $\bar{\mathbf{v}}_n^k$, the values of e_d^k and e_q^k corresponding to the synchronous machine connected to bus n is calculated as

$$\begin{bmatrix} e_d^k \\ e_q^k \end{bmatrix} = \mathbf{K}_{\mathscr{P}} \bar{\mathbf{v}}_n^k. \tag{33}$$

By recalling (24), i_d^k and i_q^k is calculated from e_d^k and e_q^k as

$$\begin{bmatrix} i_d^k \\ i_q^k \end{bmatrix} = \begin{bmatrix} \mathcal{Z}_{dd}^k & \mathcal{Z}_{dq}^k \\ \mathcal{Z}_{qd}^k & \mathcal{Z}_{qq}^k \end{bmatrix}^{-1} \left(\begin{bmatrix} \mathcal{V}_d^{k-1} \\ \mathcal{V}_q^{k-1} \end{bmatrix} - \begin{bmatrix} e_d^k \\ e_q^k \end{bmatrix} \right). \tag{34}$$

With the computed value of i_d^k, i_{fd}^k is calculated as

$$i_{fd}^k = \frac{e_{fd}^k + \frac{2}{\Delta t} \left(H_{L_{fd}}^{k-1} L_{fd} + \left(i_d^k - H_{L_{ad}}^{k-1} \right) L_{ad} \right)}{R_{fd} + \frac{2}{\Delta t} \left(L_{fd} + L_{ad} \right)}. \tag{35}$$

Since all the currents and voltages corresponding to the synchronous machine are computed, the history terms which are necessary for the consecutive time step can be updated as

$$H_{L_l}^k = 2i_d^k - H_{L_l}^{k-1} \tag{36}$$

$$H_{L_{ad}}^k = 2\left(i_d^k - i_{fd}^k \right) - H_{L_{ad}}^{k-1} \tag{37}$$

$$H_{L_{fd}}^k = 2i_{fd}^k - H_{L_{fd}}^{k-1} \tag{38}$$

$$H_{L_q}^k = 2i_q^k - H_{L_q}^{k-1}. \tag{39}$$

It is easy to observe that the updating rules (31), (32) used in the backward sweep and the models (33)–(39) which are used in the forward sweep are inclusive in nature and do not require any prediction or correction process for every time step k.

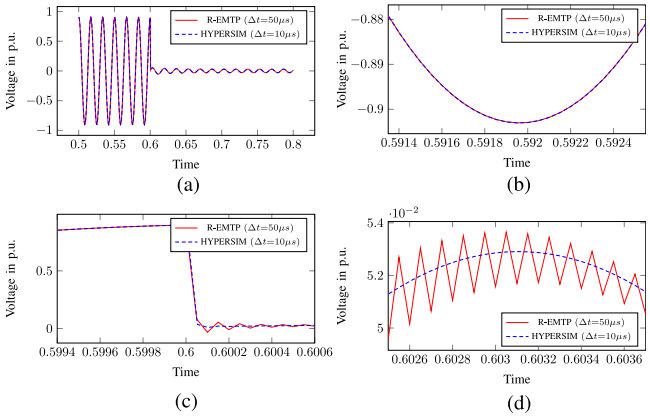

Fig. 7. Instantaneous voltage at bus 4 in 5 bus system. (a) v_4^a from 0.5–0.8 s. (b) v_4^a from 0.99075–0.99195 s. (c) v_4^a from 0.5994–0.6006 s. (d) v_4^a from 0.6025–0.6037 s.

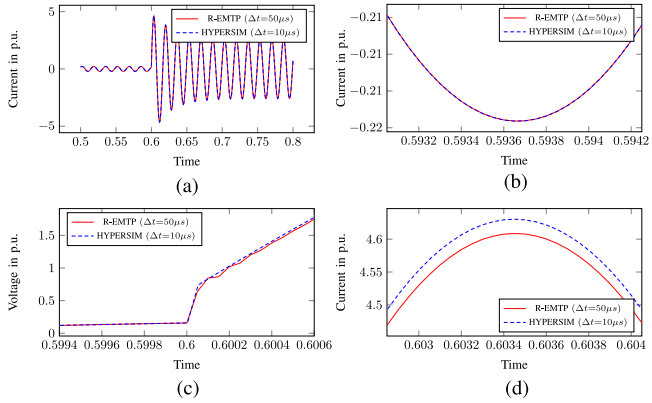

Fig. 8. Instantaneous current at line {4, 5} in 5 bus system. (a) $i^a_{\{4,5\}}$ from 0.5–0.8 s. (b) $i^a_{\{4,5\}}$ from 0.59305–0.59425 s. (c) $i^a_{\{4,5\}}$ from 0.5994-0.6006 s. (4) $i^a_{\{4,5\}}$ from 0.60285–0.60405 s.

V. Results

A. Validation of Radial EMTP

The proposed radial EMTP algorithm and the synchronous machine interfacing technique is validated in this section. This algorithm is coded in MATLAB and tested with 5-bus and 22-bus radial systems. For both of the 5-bus and 22-bus radial distribution test systems, the time step, Δt is set as 50 μs in the proposed radial EMTP approach. To validate the accuracy of the transient solution provided by the proposed radial EMTP, both the 5-bus and 22-bus test systems are implemented in Opal-RT's HYPERSIM with a time step of 10 μs and its transient solutions are compared against results of the proposed radial EMTP. A smaller time step is used for HYPERSIM in order to evaluate whether the transient solution from the proposed radial EMTP, even with coarser time steps, is able to match the results of professional-grade simulators with smaller time steps.

1) 5-Bus Radial Microgrid System: The network information of the 5-bus radial system is adopted from [26]. It is considered that two synchronous generators are the sources of electric power and they are connected to buses 1 and 3. The shafts of both the machines are driven with a constant speed of 376.99 rd/s such that the supply frequency is maintained at 60 Hz. The field windings of both the machines are supplied by constant voltage source of 0.0793 pu. The performance of the radial EMTP algorithm is tested by introducing a three phase fault in bus 5 at time instant 0.6 s. The transient solutions from the proposed radial EMTP (with $\Delta t = 50$ μs) and from Opal-RT's HYPERSIM (with $\Delta t = 10$ μs) are obtained for the simulation period from 0 to 1 s.

The instantaneous values of phase a voltage at bus 4, v_4^a, and phase a current flow at line {4,5}, $i^a_{\{4,5\}}$, are obtained using the radial EMTP and plotted in Figs. 7 and 8, respectively, and compared with the values obtained from HYPERSIM. Fig. 7(a) shows the bus 4 voltage values of phase a from 0.5 to 0.8 s and the plots given in (b)–(d) of Fig. 7 zoom this voltage signal between the time period from 0.59135 to 0.59255 s, 0.5994 to 0.6006 s, and 0.6025 to 0.6037 s, respectively. Similarly, the current values of phase a at line {4,5} from 0.5 to 0.8 s is plotted in Fig. 8(a) and the zoomed portion at time periods 0.59305 to 0.59425 s, 0.5994 to 0.6006 s, and 0.60285 to 0.60405 s are plotted in Fig. 8(b), (c), and (d), respectively. From these figures, it is observed that the calculated values of bus voltage and line current with the proposed radial EMTP are a close match with the solution obtained from HYPERSIM with $\Delta t = 10$ μs. Even though ripples are observed in Fig. 7(d) with a maximum deviation of about 1×10^{-3} pu, they closely follow the transient solution provided by HYPERSIM and they align with them after 0.61 s. Also, the maximum amount of deviation between the values provided by HYPERSIM and the radial EMTP solution noticed in Fig. 8(d) is about 0.5% (0.02 pu). The deviations observed in Figs. 7(d) and 8(d) are quite negligible and this error is due to the simplification of inductor and capacitor models with the trapezoidal rule of integration.

2) 22-Bus Radial Distribution System: The load data and line data for the 22-bus radial distribution system are taken from [18] and its line diagram is already shown in the previous section as Fig. 4. A three phase synchronous generator is considered to be supplying power from bus 1. The data for this generator are extracted from [27]. The supply frequency of this test system is considered to be 50 Hz. To create transients in the network, a three phase fault is initiated at Bus 13 in the time instant of 1 s. The simulation is carried out from 0 to 1.5 seconds with $\Delta t = 50$ μs for the proposed radial EMTP and $\Delta t = 10$ μs for Opal-RT's HYPERSIM.

The instantaneous voltage values of phase a at bus 11, v_{11}^a is plotted in Fig. 9(a) for the time period between 0.9 to 1.2 s and it is zoomed in the time periods 0.99075 to 0.99195 s, 0.9994 to 1.0006 s, and 1.0035 to 1.0047 s in Fig. 9(b), (c), and (d), respectively. In a similar way, Fig. 10(a) displays the instantaneous values of phase a current flow in line {11,13}, $i^a_{\{11,13\}}$ for the period of time between 0.9 to 1.2 s, and Fig. 10(b), (c), and (d) plot its zoomed part in the time periods 0.99305 to 0.99425 s, 0.9994 to 1.0006 s, and 1.0048 to 1.006 s, respectively. From these results, it can be concluded that the proposed radial EMTP provides almost identical results as compared to the transient solution provided by HYPERSIM with a much smaller time step, except for the minor deviations observed in Figs. 9(d)

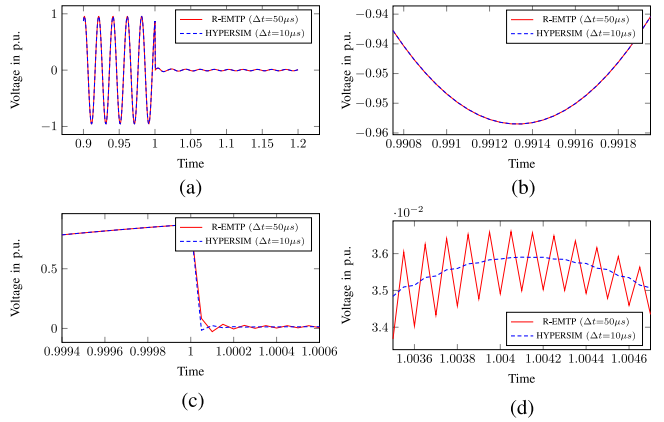

Fig. 9. Instantaneous voltage at bus 11 in 22 bus system. (a) v_{11}^a from 0.9–1.2 s. (b) v_{11}^a from 0.99075–0.99195 s. (c) v_{11}^a from 0.9994–1.0006 s. (d) v_{11}^a from 1.0035–1.0047 s.

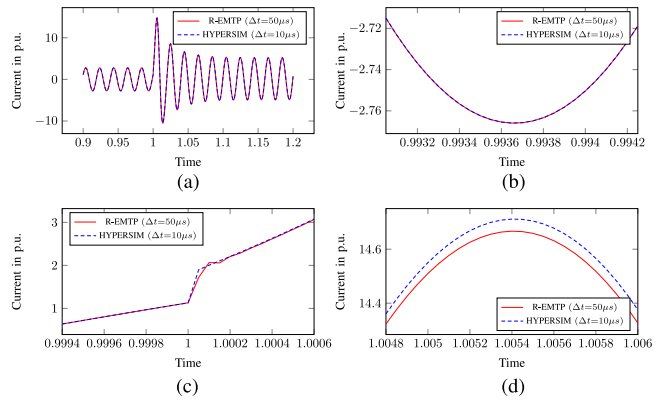

Fig. 10. Instantaneous current at line {11, 13} in 22 bus system. (a) $i_{\{11,13\}}^a$ from 0.9–1.2 s. (b) $i_{\{11,13\}}^a$ from 0.99305–0.99425 s. (c) $i_{\{11,13\}}^a$ from 0.9994–1.0006 s. (4) $i_{\{11,13\}}^a$ from 1.0048–1.006 s.

and 10(d). The key advantage is that radial EMTP takes less computation resources and hence it can be easily incorporated in small computing machines while obtaining similar results as from the conventional EMTP for the same given time step. From timing measurements conducted during our experiments, we observed that conventional EMTP requires about 2.3 times more computation time than radial EMTP when both EMTPs use the same time step. This is because the computational complexity of the radial EMTP is far lesser than that of conventional EMTP for solving radial distribution networks.

B. Evaluation of Data Manipulation Attack Detection

The proposed attack detection technique is evaluated using the 5-bus microgrid system and 22-bus distribution system which were previously used for validating the radial EMTP. Typical micro-PMUs which are used in distribution systems have an accuracy level of $\pm 10^{-4}$ pu for voltage magnitude measurements and can transmit 1 or 2 samples per cycle [28]. To be on the conservative side, the noise in the measurement values in both the 5-bus and 22-bus systems are considered to have a zero mean Gaussian distribution with a standard deviation of 2×10^{-4} pu

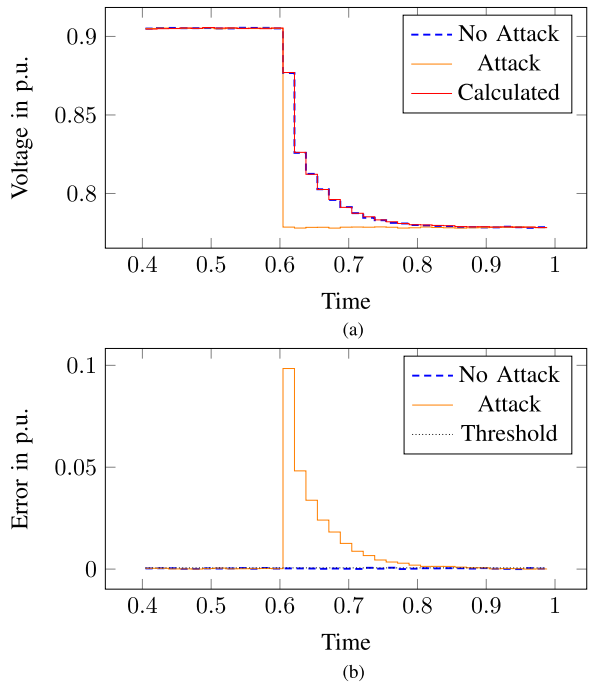

Fig. 11. Voltage magnitude and error at bus 1 in 5 bus system. (a) Voltage magnitude at bus 1. (b) Error.

and at least one voltage magnitude measurement is available per cycle.

1) 5-Bus Radial Microgrid System: The simulation for the 5-bus microgrid system is executed for a period of 1 s. Its voltage magnitude measurements are updated at the rate of 60 samples per second. Two scenarios are considered to verify the proposed detection technique: No-attack scenario and Attack scenario. In the no-attack scenario, a legitimate load with the values of $\mathbf{P} = 2.0889$ pu and $\mathbf{Q} = 7.3879 \times 10^{-3}$ pu is added at bus 5 at time instant 0.6 s, in addition to its existing loads. For the attack scenario, the voltage magnitude measurements from bus 1 to bus 5 are manipulated to falsely inject the effect of a new load addition (of $\mathbf{P} = 2.0889$ pu and $\mathbf{Q} = 7.3879 \times 10^{-3}$ pu) at bus 5. Such an attack is considered to be initiated at the time instant of 0.6 s where the voltage magnitude measurement at Bus 1 is reduced from 0.9 pu to 0.78 pu.

Such an attack can be executed by calculating the amount of voltage change required to fake the given load addition as detailed in Section 4.1.1. In this manner, it is found that the voltage magnitude at bus 1 needs to be changed to 0.78 pu from its original value of 0.9 pu in order to account for the additional load at bus with $\mathbf{P}$ and $\mathbf{Q}$ values of 2.0889 pu and 7.3879×10^{-3} pu, respectively.

Using the proposed radial EMTP, the bus 1 voltage magnitude values are calculated and plotted in Fig. 11(a) along with the measured values under no-attack and attack scenarios. Due to the system dynamics, it takes a period of 0.3 s for the voltage at bus 1 to transient from its initial value of 0.85 pu to reach the steady-state value to 0.76 pu. The error deviations between the calculated and measured values in both no-attack and attack scenarios is plotted in Fig. 11(b). The calculated values are in close

TABLE II
TRUE POSITIVE RATE AND FALSE POSITIVE RATE OF THE PROPOSED DETECTION TECHNIQUE IN 5-BUS SYSTEM

% of Load	20	30	40	50	60	70	80	90	100	110	120	130	140
TPR	80	98	100	100	100	100	100	100	100	100	100	100	100
FPR	0	0	0	0	0	0	0	0	0	0	0	0	0

agreement with the measured values in the no-attack scenario as the maximum error is around 0.0024 pu. This accounts for the injected zero mean Gaussian noise with 2×10^{-4} pu standard deviation.

The detection threshold is set as 6×10^{-4} pu to consider 99.73% of the variations caused due to the noise injection. In the attack case, the maximum error is around 0.027 and the threshold violation occurs for a time span of about 0.1 s. As the measuring devices are operated at a sampling rate of 60 samples per second, at least eleven threshold violations can be observed in the attack scenario.

With these considerations, the threshold value, τ is set as 6×10^{-4} pu and η which is the minimum number of consistent threshold violations that raises the alarm is set as 11. To analyze the detection rate of the proposed technique, the 5-bus system is subjected to attack and no-attack scenarios for 100 Monte Carlo repetitions each. The total number of detections in the 100 attack scenario repetitions is defined as true positive rate (TPR) and the total number of detections in the 100 no-attack scenario repetitions is defined as false positive rate (FPR). For this analysis, we simulate attacks with different magnitudes of false load injection. For this scenario and analysis, a 100% load change corresponds to the addition of $\mathbf{P} = 2.0889$ pu and $\mathbf{Q} = 7.3879 \times 10^{-3}$ pu at bus 5. The values of TPR and FPR are calculated for the percentage of load change varying from 20% to 140% with incremental steps of 10% and the results are tabulated in Table II. From these results, it can be seen that the proposed technique does not generate any false alarms (as FPR is 0% for all the load changes) and provides a 100% detection rate if the load change is more than 40%.

2) 22-Bus Radial Distribution System: The 22-bus distribution system is simulated from the period 0 to 1.5 s. The measured voltage magnitude values are considered to be refreshed once in every 20 ms. Under the no-attack scenario, it is considered that a new load is added at bus 13 at time instant 1 s whereas the loads remain in the previous values. The values of $\mathbf{P}$ and $\mathbf{Q}$ that are newly added to bus 13 are 2.1345 pu and 7.7881×10^{-3} pu, respectively. During the attack scenario, the measurements are manipulated such that it is perceived that a new load is added at bus 13 with the values of $\mathbf{P}$ and $\mathbf{Q}$ as 2.1345 pu and 7.7881×10^{-3} pu, respectively. It is considered that with such an attack, the voltage magnitude measurement at bus 1 is reduced from 1 to 0.907 pu in order to reflect a fake load addition at bus 13. This attack is assumed to be started at time instant 1 s.

Since a significant load change is observed in both no-attack and attack scenarios, the values of voltage magnitude measurements at bus 1 are calculated for the observed load change using the proposed radial EMTP technique. The measured values of voltage magnitude at bus 1 in both no-attack and attack scenarios is plotted in Fig. 12(a) along with the calculated values using proposed radial EMTP. It is observed that, in no-attack scenario, the voltage value at bus 1 takes around 0.4 s from its initial value of 1.09 pu to settle in its final value of 1 pu. The error difference between the calculated and measured values of bus 1 voltage magnitude is plotted in Fig. 12(b) for both no-attack and attack scenarios. To account for the 99.73% Gaussian noise variations, the detection threshold is set as 6×10^{-4} pu.

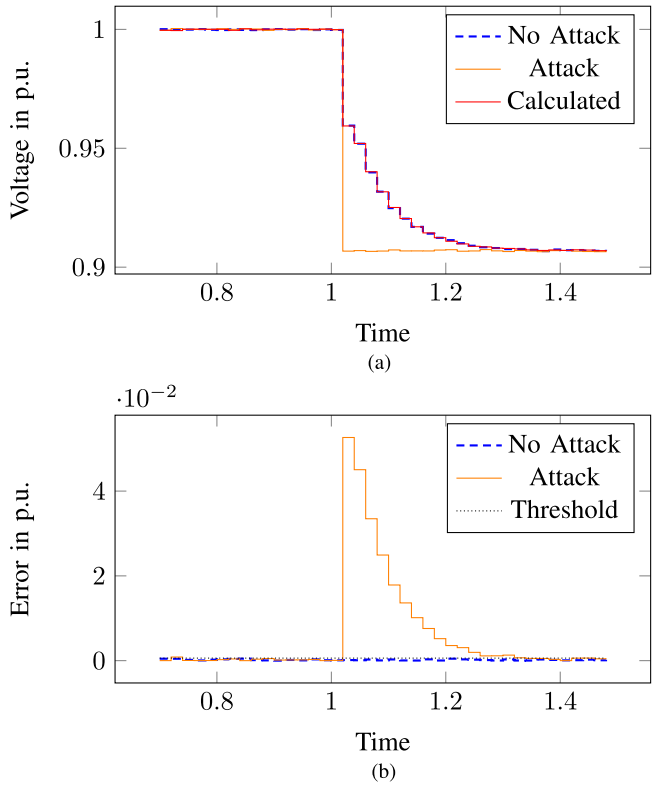

Fig. 12. Voltage magnitude and error at bus 1 in 22 bus system. (a) Voltage magnitude at bus 1. (b) Error.

In the no-attack scenario, the deviations between the calculated and measured values does not exceed 4.6×10^{-4} pu after 1 s time instant as the legitimate measurements follow the system dynamics which is realized with the values calculated using radial EMTP. In contrast, during the attack scenario, as the measurements do not reflect the actual system dynamics, the error value shoots to a maximum value of around 5.26×10^{-2} pu and threshold violations happen in at least 11 measurement samples, roughly for a period of 0.2 seconds. Thus, the proposed detection technique is able to distinguish whether the measurements are manipulated or not using the transient components present in the measurements.

For evaluating the TPR and FPR of the proposed detection scheme in the 22-bus system, τ and η are set to be 6×10^{-4} pu

TABLE III
TRUE POSITIVE RATE AND FALSE POSITIVE RATE OF THE PROPOSED DETECTION TECHNIQUE IN 22-BUS SYSTEM

% of Load	20	30	40	50	60	70	80	90	100	110	120	130	140
TPR	76	97	100	100	100	100	100	100	100	100	100	100	100
FPR	0	0	0	0	0	0	0	0	0	0	0	0	0

and 11, respectively. To obtain the values of TPR and FPR under different attack levels, we define that 100% load change at bus 13 is considered to be $\mathbf{P} = 2.1345$ pu and $\mathbf{Q} = 7.7881 \times 10^{-3}$ pu. In the 22-bus system, attack and no-attack scenarios are repeated for 100 Monte Carlo simulations for the amount of change in load from 20% to 140% in step wise manner with step size of 10%. The values of TPR and FPR found in each of the load changes are tabulated in Table III. The results obtained for the 22-bus system are similar to the TPR and FPR values obtained in the 5-bus system as the FPR of the proposed technique is 0%, and hence, it will not create any false alarms even for smaller load changes. The TPR of the proposed technique is 100% for a load change that is more than 40%. Thus, it will not miss any of the data manipulation attacks that fakes a load change higher than 40% of the above specified values of $\mathbf{P}$ and $\mathbf{Q}$.

VI. CONCLUSION

This article presented a detection scheme for data manipulation attacks against measurements in distribution systems. A three phase radial EMTP technique is proposed which follows a BFS-based approach by exploiting the topographical nature of distribution systems. This article also proposed a three phase synchronous generator model which is directly compatible with the radial EMTP algorithm. Such a model does not need to predict and correct the speed voltages in both d- and q-axes as they are incorporated directly into the proposed model. The proposed technique is evaluated on 5-bus and 22-bus distribution systems to show that the radial EMTP and the proposed synchronous machine model provides similar results as conventional EMTP, and to validate the proposed attack detection mechanism.

REFERENCES

[1] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, 2009, pp. 21–32.

[2] S. Soltan, P. Mittal, and H. V. Poor, "Line failure detection after a cyber-physical attack on the grid using Bayesian regression," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 3758–3768, Sep. 2019.

[3] J. R. R. Kumar, B. Sikdar, and D. Kundur, "Three-phase radial EMTP and stealthy attack detector for distribution systems," in *Proc. IEEE Int. Conf. Power Electron., Drives Energy Syst.*, 2020, pp. 1–4.

[4] J. R. K. R. and B. Sikdar, "Detection of stealthy cyber-physical line disconnection attacks in smart grid," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4484–4493, Sep. 2021.

[5] H. W. Dommel, "Digital computer solution of electromagnetic transients in single-and multiphase networks," *IEEE Trans. Power App. Syst.*, vol. PAS-88, no. 4, pp. 388–399, Apr. 1969.

[6] A. Ametani, "Electromagnetic transients program: History and future," *IEEJ Trans. Elect. Electron. Eng.*, vol. 16, no. 9, pp. 1150–1158, Sep. 2021.

[7] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in distributed power systems," *Proc. IEEE*, vol. 105, no. 7, pp. 1367–1388, Jul. 2017.

[8] Q. Dai, L. Shi, and Y. Ni, "Risk assessment for cyberattack in active distribution systems considering the role of feeder automation," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3230–3240, Jul. 2019.

[9] R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2871–2881, May 2019.

[10] P. Zhuang, R. Deng, and H. Liang, "False data injection attacks against state estimation in multiphase and unbalanced smart distribution systems," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6000–6013, Nov. 2019.

[11] M. Chlela, G. Joos, and M. Kassouf, "Impact of cyber-attacks on islanded microgrid operation," in *Proc. Workshop Commun. Comput. Control Resilient Smart Energy Syst.*, New York, NY, USA:ACM, 2016, pp. 1–5.

[12] S. Liu, X. Wang, and P. X. Liu, "Impact of communication delays on secondary frequency control in an islanded microgrid," *IEEE Trans. Ind. Electron.*, vol. 62, no. 4, pp. 2021–2031, Apr. 2015.

[13] M. Chlela, G. Joos, M. Kassouf, and Y. Brissette, "Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2016, pp. 1–5.

[14] M. Rekik, Z. Chtourou, C. Gransart, and A. Atieh, "A cyber-physical threat analysis for microgrids," in *Proc. 15th Int. Multi-Conf. Syst., Signals Devices*, 2018, pp. 731–737.

[15] X. Zhang, X. Yang, J. Lin, and W. Yu, "On false data injection attacks against the dynamic microgrid partition in the smart grid," in *Proc. IEEE Int. Conf. Commun.*, 2015, pp. 7222–7227.

[16] 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 *Proc. IEEE PES/IAS PowerAfrica*, 2018, pp. 533–538.

[17] 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 Trans. Ind. Electron.*, vol. 66, no. 2, pp. 1543–1551, Feb. 2019.

[18] M. Ramalinga Raju, K. Ramachandra Murthy, and K. Ravindra, "Direct search algorithm for capacitive compensation in radial distribution systems," *Int. J. Elect. Power Energy Syst.*, vol. 42, no. 1, pp. 24–30, 2012.

[19] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[20] J. Fraleigh, R. Beauregard, and V. Katz, *Linear Algebra*. Reading, MA, USA: Addison-Wesley, 1994.

[21] Y. Xia, Y. Chen, Y. Song, S. Huang, Z. Tan, and K. Strunz, "An efficient phase domain synchronous machine model with constant equivalent admittance matrix," *IEEE Trans. Power Del.*, vol. 34, no. 3, pp. 929–940, Jun. 2019.

[22] V. Brandwajn, "Synchronous generator models for the simulation of electromagnetic transients," Ph.D. dissertation, Dept. Elect. Eng., Univ. Brit. Columbia, Vancouver, BC, Canada, 1977.

[23] "*IEEE Guide for Synchronous Generator Modeling Practices and Parameter Verification with Applications in Power System Stability Analyses*," IEEE Standard 1110-2019, (*Revision of IEEE Standard 1110-2002*), 2020, pp. 1–92.

[24] P. Kundur, *Power System Stability and Control (EPRI Power System Engineering Series)*. New York, NY, USA: McGraw-Hill, 1994.

[25] G. Valverde, E. Kyriakides, G. T. Heydt, and V. Terzija, "On-line parameter estimation of saturated synchronous machines," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2011, pp. 1–6.

[26] S. Eberlein, A. Heider, and K. Rudion, "Modelling and control optimization of diesel synchronous generators in LV microgrids," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. Europe*, 2018, pp. 1–6.

[27] R. Wamkeue, C. Jolette, A. B. M. Mabwe, and I. Kamwa, "Cross-identification of synchronous generator parameters from RTDR test time-domain analytical responses," *IEEE Trans. Energy Convers.*, vol. 26, no. 3, pp. 776–786, Sep. 2011.

[28] A. von Meier, E. Stewart, A. McEachern, M. Andersen, and L. Mehrmanesh, "Precision micro-synchrophasors for distribution systems: A summary of applications," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2926–2936, Nov. 2017.