IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 4, 2019, accepted May 26, 2019, date of publication May 30, 2019, date of current version June 12, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2920080

Remote Detection and Identification of Illegal Consumers in Power Grids

AHMED BIN-HALABI, (Student Member, IEEE), ADNAN NOUH, AND MOHAMMAD ABOUELELA

Electrical Engineering Department, College of Engineering, King Saud University, Riyadh 11421, Saudi Arabia

Corresponding author: Ahmed Bin-Halabi (434108017@student.ksu.edu.sa)

This work was supported by the Deanship of Scientific Research at King Saud University through the initiative of DSR Graduate Students Research Support (GSR).

ABSTRACT Electricity theft is a common problem in electric power systems around the world. It causes heavy economic losses and badly affects the reliability of the power grid. One of the most common and simplest methods of stealing electricity is tapping energy directly from the overhead power feeder. The other most common method of theft is the tampering with meters to reduce the recorded consumption by illegal ways. In this paper, we present a cost-effective remote detection and identification method for detecting illegal electricity consumption. It also identifies the illegal user in real time without any pre-processing or extensive analysis of a huge amount of collected data. Moreover, it preserves the privacy of customers by destroying the high-resolution data of instantaneous power consumption collected from customers' meters. The system can detect suspicious consumer(s) online and sends notifications to the utility control center with the ID number(s) of the suspicious meter(s) or the amount of load that has been tapped to the power feeder within the area served by a single distribution transformer. The extensive simulations using Simulink were conducted to validate the proposed scheme. For further validation of the scheme, hardware-in-the-loop (HIL) simulation was conducted using three microcontroller-based meters and Simulink environment. The results of both types of experiments showed that the proposed scheme can successfully detect and identify fraudulent users in real time.

INDEX TERMS AMR, electricity theft, fraudulent user, remote detection, running difference.

I. INTRODUCTION

A. CONTEXT

Although electricity theft is a global problem, the developing countries in general have the highest rate [1]. The financial losses incurred by power utilities due to non-technical losses (NTLs) that are caused by electricity theft result in shortage of funds for not only improvement and investment in the capacity of power grid, but also for fuel supply [2]. Along with the financial losses, electricity theft can also result in unexpected rising demand that could overload the grid and the power plants at peak hours.

One of the most common and simplest methods of stealing electricity is tapping energy directly from the overhead power feeder. The other most common method of theft is the tampering with meters [1]. It has been very difficult for power utilities to detect and identify the people responsible for electricity theft. The dissemination of smart grid concept and the implementation of advanced metering infrastructures (AMIs) result in power grids with many digitally interconnected assets that allow full remote control and monitoring. Bidirectional communication between assets and power utility can enable better grid management. At the same time, the widespread use of cybernetic systems opens the door to hackers and cyber attackers [3].

The associate editor coordinating the review of this manuscript and approving it for publication was Bohui Wang.

B. RELATED WORK

A variety of electricity theft detection schemes have been proposed in the literature. In [3], a data-based method for energy theft detection is proposed. Data collected during one and a half years from smart meters are clustered using Gustafson-Kessel fuzzy algorithm to extract typical consumption behavior models. The new data samples are classified as malign if they are significantly away from the extracted typical models. In [4], a fuzzy logic based method is proposed to determine the total suspicion value of a set of customers in area of increased total energy losses. Historical

data of monthly billed energy for about 15 years is used for the analysis and detection of the cause of the losses. This is for original customers, but not for feeder-tapped load detection. Another fuzzy-based scheme is proposed in [5].

In [6], a parallelized multi-level algorithm is proposed to identify fraudulent consumers by encoding collected data in order to be simplified for the succeeding support vector machine (SVM) classification. More other SVM-based schemes are proposed in [7]–[10]. A SVM-based NTL detect-ion improved by fuzzy inference system is proposed in [11].

The utilization of artificial neural networks (ANNs) to detect energy theft is reported in [12]–[14]. In [12], a wide and deep convolutional neural networks (CNN) model is proposed for theft detection in smart grids. The system proposed in [13] consists of three parts. The first part classifies the customers with similar consumption curves by the use of self-organizing maps and genetic algorithms. The second part uses autoregressive integrated moving average (ARIMA) models to perform forecasting for monthly demand. The last part performs pattern recognition using ANN to detect the fraudulent users. In [14] two types of illegal consumption are defined:

(1) All customer's loads are supplied illegally but in a portion of day.

(2) Part of customer's loads is supplied illegally all the day.

Two methods are combined to detect the two types of illegal consumption; the first one classifies the consumption pattern of customers to detect the first type of illegal consumption based on probabilistic ANN, and the second method is based on Levenberg-Marquardt algorithm to detect the second type.

There are several different techniques reported in the literature for this problem. In [15], two linear programming-based NTLs detection algorithms are proposed. The algorithms evaluate the anomaly coefficients of studied customers' energy consumption behavior to detect energy theft and faulty smart meters in smart grid environment. The same work is continued in [16] with experimental additions. In [17], a statistical method based on Tukey's control charts is used to analyze customers' time series to estimate the suspicious customers. The series are formed by using historical monthly data measurements of electricity consumption. In [18], a P-median model is used to allocate power-quality monitors in distribution systems to identify NTLs. The rough set theory is used in [19] for the estimation of set size and for determining the members of set to be checked, in order to detect fraud committed by customers. A data-driven energy theft detection scheme for AMI networks based on random matrix theory is proposed in [20]. The authors proposed the use of distributed meter data management solution along with the augmented matrix and split window techniques for the identification of fraudulent customers and regions. In [21], a relative entropy based method is proposed for electricity theft detection in AMI networks. In [22], a three-stage multi-view stacking ensemble machine learning model based on hierarchical time series feature extraction method is proposed to solve the anomaly detection problem. Anomaly detection of power consumption, essentially including electricity theft and unexpected energy loss.

A survey of artificial intelligence techniques used for NTLs detection is reported in [23]. Recent reviews of various schemes proposed for the detection of electricity theft are published in [24]–[27].

All the above discussed methods are based on historical data collection for certain periods of time. However, the remote real-time detection and identification of illegal users is impossible through these methods because they need data analysis and statistical operations on the historical data. Therefore, some remote real-time detection techniques have been proposed in the literature based on automatic meter reading (AMR) systems.

In [28], an AMR-based scheme for remote detection of illegal electricity consumption via PLC is proposed. Each customer will be equipped, in addition to the existing main AMR system, with a new combination of PLC modem and energy metering chip. Each new unit, which forms like an additional AMR system, will be installed at the connection point between main distribution line and customer's branch line as shown in Fig. 1. Installing additional PLC-meter unit for each customer in the grid means doubling the number of AMR systems which will be costly. Moreover, doubling the PLC modems will double the data traffic in the communication channel and may increase the interference level in the system.

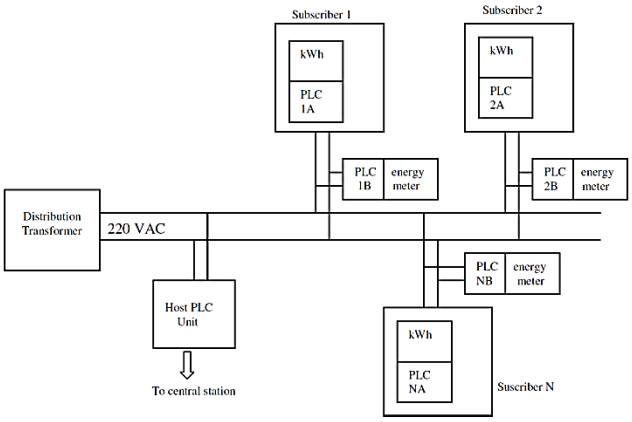

FIGURE 1. The remote detection method proposed in [28].

In [29], the authors proposed a remote detection method based on smart meter. Smart meter is suggested in [29] instead of conventional AMR system because it has the capability of remote disconnection. During the detection process, a central smart meter disconnects electricity to all customers and sends a low voltage (2 V) AC signal of high frequency (150 kHz) through the main distribution line and calculates (using Ohm's law) the impedance of the line. The illegal consumption can be detected in this method by using the low

voltage characteristics of power line, where the calculated impedance of each line that connects two smart meters to each other is compared with a reference impedance value that was previously obtained at the time of grid installation. Any difference between the two impedance values implies illegal electricity consumption. The main disadvantage of this scheme is that it must disconnect electricity to all customers to detect whether illegal usage of electricity is exist in a certain line or not.

To avoid the disconnection problem in [29], the authors in [30] proposed adding what they called a smart resistance to each customer's smart meter. The resistance is electronically controlled to regulate its value and it is preceded by a switch, and both the resistance and the preceding switch are shunted together with another parallel switch as shown in Fig. 2. Each customer's meter sends its consumption reading to the substation and the total sum of all readings is compared with the reading of the central meter at the substation. If there is a difference between them, illegal consumption will be confirmed. In this case, the AMR system will send commands to all smart meters to check illegal consumption. When the command signal is received by the smart meter it switches S1 off and S2 on to connect the smart resistance. The values of voltage and current corresponding to the selected smart resistance value are calculated and stored in the system. The smart resistance is then disconnected after switching S1 on.

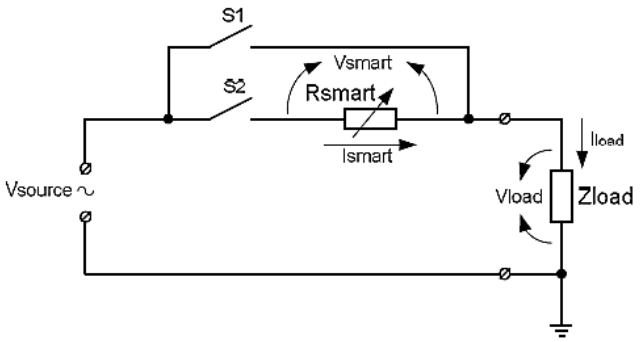

FIGURE 2. The smart resistance circuit added to smart meter that proposed in [30].

Since the smart resistance is connected in series with the customer's load, the same current should pass through them in normal condition. However, if the meter is shunted for electricity theft and when S1 is open and S2 is closed during checking phase, the currents will not be the same which implies electricity theft. The main disadvantage of this method is that the smart resistance, which is an electronically controlled resistor, must be capable to handle high currents to supply customer's load, so it may be bulky and rather costly.

Another method that allows detecting illegal consumption remotely but with customers disconnection is proposed in [31]. In this method, two types of modified smart meters are used. One type is installed at each customer side and called terminal smart meter (TSM), and the other type is installed at each node of power grid and called gateway smart meter (GSM), as shown in Fig. 3. The GSM can entirely connect/disconnect electricity to all customers connected to the same node. It contains two energy metering modules (EM1 and EM2), AC/AC regulator (buck-boost converter), testing voltage generator (TVG), in addition to a switch. The block diagram of the TSM is shown in Fig. 4. Two types of inspection are performed for detection in this method. The first type is to check the existence of a shunt connection across the meter, where the AC/AC regulator inside the TSM reduces the input voltage for a short period of time and the EM2 senses the output voltage of the TSM. If there is no illegal shunt installed, the output voltage will be less than the input voltage due to the AC/AC regulation. However, if the TSM is shunted, the output voltage will be equal to input voltage (i.e. no change).

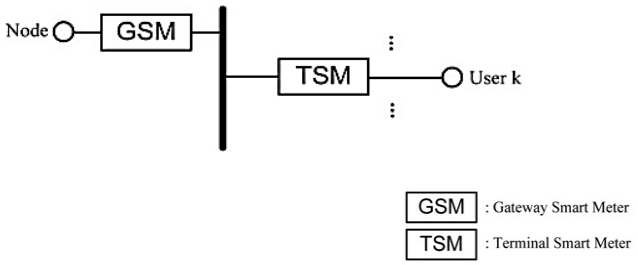

FIGURE 3. The system proposed in [31].

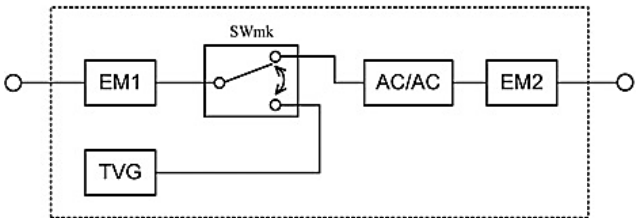

FIGURE 4. The TSM meter proposed in [31].

The second type of test is to check the existence of any illegal branched connections before the TSMs. To detect the branched connection, the GSM disconnects from the grid and the TSM internal switch changes to the TVG source; both of the operations are performed in a very short period. This will convert the TSM into a high-frequency low-voltage source. Then, the GSM measures the current and voltage and calculates the impedance of the power line between the node and the TSM. If the calculated impedance is different than a pre-calculated normal condition value, illegal connection is confirmed. To inspect the other lines or customers, this process should be repeated for each customer in order. Although this method can work, but it is costly. In addition to the number of components needed for one TSM, the AC/AC buck-boost converter for high power applications (whole customer load) is generally bulky and expensive.

C. MOTIVATION OF THE STUDY

Although real-time detection of illegal consumption is preferable by any utility company, it is avoided due to the high cost of most solutions proposed in the literature. Motivated

TABLE 1. Qualitative comparison of the proposed method with several existing real-time detection methods.

Scheme	Hardware extension required for energy meters	Pre-calculated parameters	Types of theft that can be detected	Customer disconnection	Cost
[28]	Additional AMR meter for each customer	None	– Meter tampering	None	High
[29]	Low-voltage high-frequency generator	Line impedance	– Direct connection to grid	All customers – at once	Medium
[30]	Smart resistance and two switches	None	– Meter tampering – Direct connection to grid	None	High
[31]	Two energy metering units per customer, test voltage generator, and AC/AC voltage regulator	Line impedance	– Meter tampering – Direct connection to grid	All customers – one at a time	High
Proposed	None	None	– Meter tampering – Direct connection to grid	Suspected only	Low

by this reason, we propose a cost-effective real-time detection method that can detect illegal electricity consumption and identify the illegal user in the real-time without any pre-processing or extensive analysis of huge amount of collected data as in [3]–[22]. Furthermore, the proposed scheme can be applied on any existing AMR system with simple and low cost additions and modifications. A qualitative comparison between the proposed method and some of the most related real-time detection methods is presented in Table 1.

II. PROPOSED SCHEME

A. SYSTEM ARCHITECTURE

In this work, a remote detection and identification method is proposed, where a central monitoring and inspection unit (MIU) is adopted for each group of customers served by one distribution transformer as shown in Fig. 5. The combination of a distribution transformer and all the customers served by it will be referred to throughout this paper as a transformer zone, or shortly, a T-Zone. Each T-Zone is monitored and controlled by its associated MIU. In Fig. 5, a T-Zone with a distribution transformer serves a number of customers, and equipped with an MIU.

The MIU measures the transformer total power supplied through the secondary feeder to the customers and, in the same time, receives instantaneous power consumption from each customer's meter via AMR system and compares the total sum of the received power values with the measured power drawn from the transformer. If there is a significant difference between them, illegal electricity consumption is confirmed, and the role of detection and identification algorithm starts.

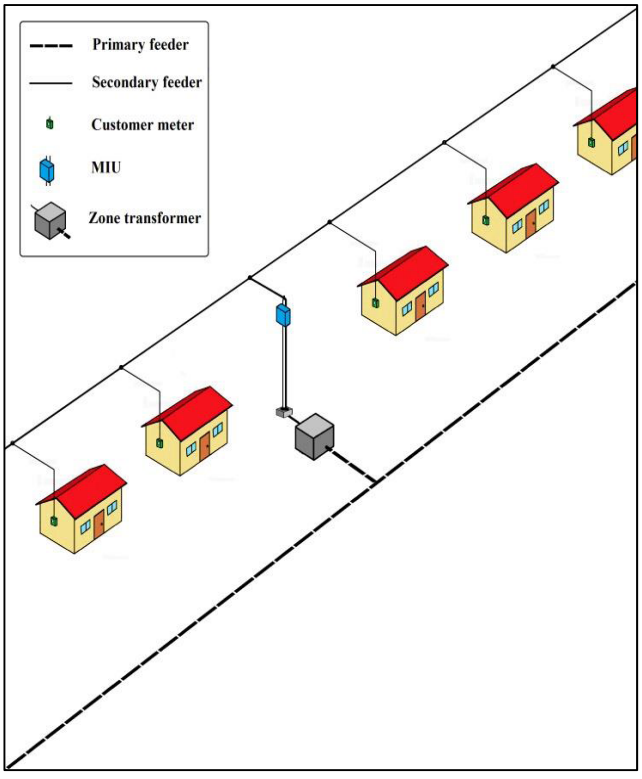

FIGURE 5. A T-Zone with the proposed system infrastructure.

B. REAL-TIME DETECTION AND IDENTIFICATION (RTDI) ALGORITHM

The proposed model is based on the following assumptions:

- Each group of customers of size N are served by one distribution transformer.
- Each customer is equipped with a smart meter or AMR system with a disconnect relay.
- Stealing energy by meter tampering typically leads to reducing the power reading of the meter than that actually being consumed.
- Direct connection to the grid causes the power drawn from distribution transformer to be greater than the total sum of the power consumptions of all customers served by that transformer.

The electricity theft or any suspicious behavior of consumption in a T-Zone can be detected by using the

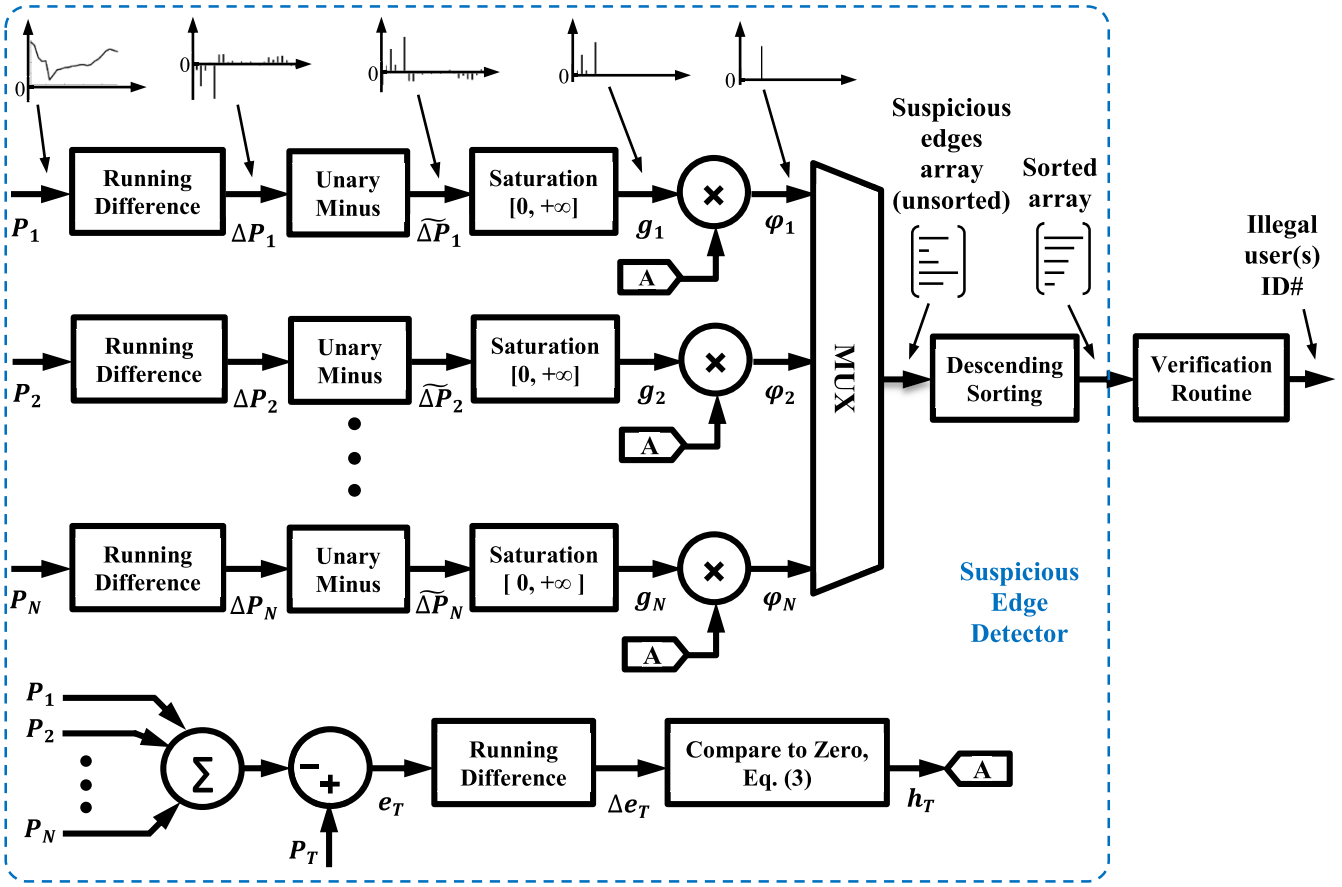

FIGURE 6. Block diagram of the proposed RTDI algorithm.

proposed real-time detection and identification (RTDI) algorithm according to the following procedure explained below.

The deviation, $e_T(t)$, between the power drawn from the distribution transformer at any instant of time t and the sum of power consumptions of all the N customers served by the transformer is calculated as follows:

$$e_T(t) = P_T(t) - \sum_{i=1}^{N} P_i(t) \tag{1}$$

where $P_T(t)$ is the actual power drawn from the distribution transformer, and $P_i(t)$ is the power consumption received from the meter of customer $i(1 \le i \le N)$.

By applying the running difference operation on (1) we get:

$$\Delta e_T(t) = e_T(t+1) - e_T(t) \tag{2}$$

where t is the sampling instant.

Since (2) may yield positive or negative values, the negative values are filtered out with zero and the positive values are masked as one using the following formula:

$$h_T(t) = \begin{cases} 1, & \text{if } \Delta e_T(t) > 0 \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

In the same way, the running difference of power consumption for customer $i(1 \le i \le N)$ is calculated as follows:

$$\Delta P_i(t) = P_i(t+1) - P_i(t) \tag{4}$$

Equation (4) may also yield positive or negative values. However, since we are concerned about the negative values because they imply reduction in the received power values, $\Delta P_i(t)$ values are negated to convert the interesting negative values into positive ones in order to find the maximum values instead of the minimum ones. The last step can be skipped if one interested in finding the minimum values instead. Hence, the negative version of $\Delta P_i(t)$ is:

$$\widetilde{\Delta P}_i(t) = -\Delta P_i(t) \tag{5}$$

The negative portion of $\widetilde{\Delta P}_i(t)$ is clipped using the following saturation formula:

$$g_i(t) = \begin{cases} \widetilde{\Delta P}_i(t), & \text{if } \widetilde{\Delta P_i(t)} > 0 \\ 0, & \text{otherwise} \end{cases} \tag{6}$$

where $g_i(t)$ is the saturated value of $\widetilde{\Delta P}_i(t)$.

The suspicious behavior of consumption for customer $i(1 \le i \le N)$ at the instant of time t (which will be referred to as suspicious edge in this paper) can be detected by multiplying (3) by (6) as follows:

$$\varphi_i(t) = h_T(t)\, g_i(t) \tag{7}$$

where $\varphi_i(t)$ is the suspicious edge for customer i at the instant of time t.

If only one suspicious customer is detected at a certain instant of time, the MIU will send a notification with the detected meter ID number to the utility control office. However, if more than one suspicious user are detected at the same instant of time t; although the likelihood of more than one user to start electricity theft within the same T-Zone at exactly the same moment is very low, an array of suspicious edges for those users can be obtained as follows:

$$\begin{bmatrix} \varphi_1(t) \\ \varphi_2(t) \\ \vdots \\ \varphi_N(t) \end{bmatrix} = h_T(t) \begin{bmatrix} g_1(t) \\ g_2(t) \\ \vdots \\ g_N(t) \end{bmatrix} \tag{8}$$

or

$$\boldsymbol{\varphi}(t) = h_T(t)\mathbf{g}(t) \tag{9}$$

The suspicious meters can be then easily identified using the indexes of the nonzero elements of φ.

In order to avoid false-positive alerts, the suspicious edges (meters) array is passed through a verification routine to confirm the illegal users and to distinguish between meter tampering and overhead feeder tapping. To confirm the actual fraudulent user(s), the MIU will send disconnection commands to only the suspicious meters in the descendingly sorted array, one by one, staring with the meter with the highest edge. After disconnecting a suspicious meter, the verification routine will check whether the power deviation e_T is affected or not. If disconnecting a meter results in reduction in both P_T and e_T, it will directly confirm that this customer has tampered with the meter to reduce his/her actual consumption. However, if the disconnection results in reduction in P_T but does not affect e_T, the customer honesty will be confirmed. If the disconnection does not affect P_T at all, regardless of e_T, this will directly confirm that the meter is bypassed.

If any illegal consumption is not detected (for any reason) by the suspicious edge detector and there still exists a significant difference between the transformer power and the aggregated power of all the meters served by the transformer, the verification routine will start the verification process to detect the consumer who is causing this difference. Therefore, all the energy theft forms will be eventually detected by the algorithm.

The block diagram of the proposed algorithm and the flowchart of the verification routine are presented in Fig. 6 and Fig. 7, respectively.

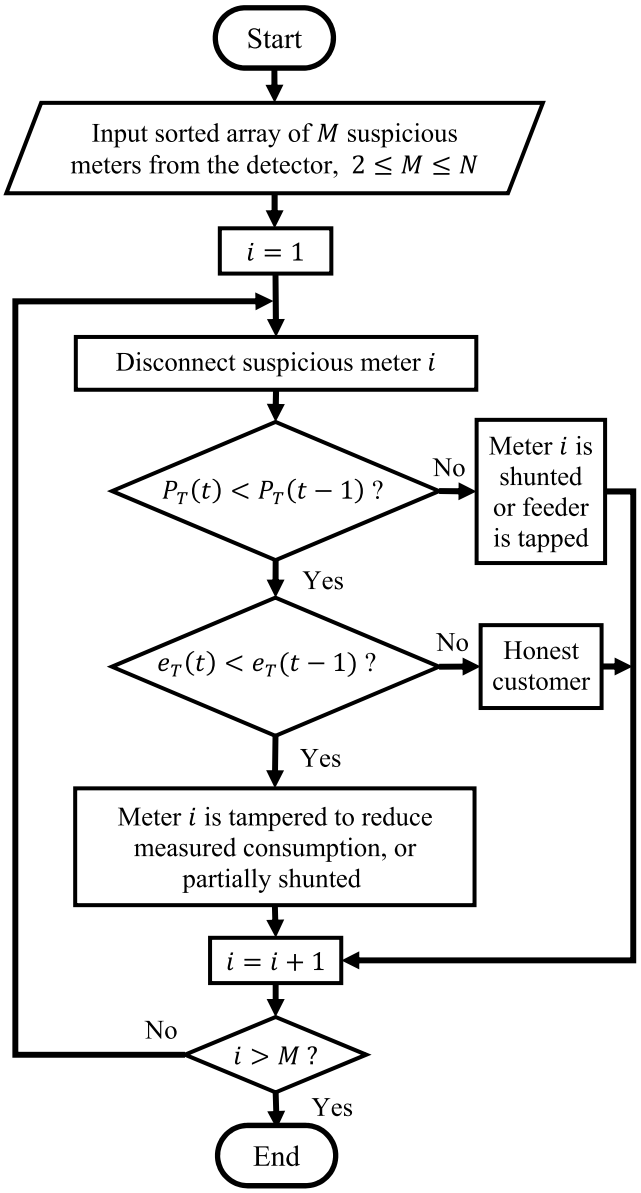

FIGURE 7. Flowchart of the verification routine.

III. EXPERIMENTATION

A. SOFTWARE SIMULATION

Matlab/Simulink environment is used to simulate the system. A T-Zone with only ten customers is considered for convenience. The developed Simulink model of power grid comprises a power substation, transmission lines, a distribution transformer, the ten customers' meters, as well as the MIU that contains the proposed RTDI algorithm. The load profiles for only five customers and the output of each processing stage of the RTDI algorithm for an arbitrary scenario of electricity theft are shown in Fig. 8.

B. HARDWARE-IN-THE-LOOP (HIL) SIMULATION

Because we are currently unable to implement the whole system on a real power grid containing all the required components of power grid such as distribution transformer, distribution lines, and a number of real customers with their power meters and loads, we performed a hardware-in-the-loop (HIL) simulation using Simulink and microcontroller boards. We have built two hardware energy meters to measure the instantaneous power consumption of two assumed customers, and we have also built a third power meter to measure the aggregated power consumed by these two customers. The

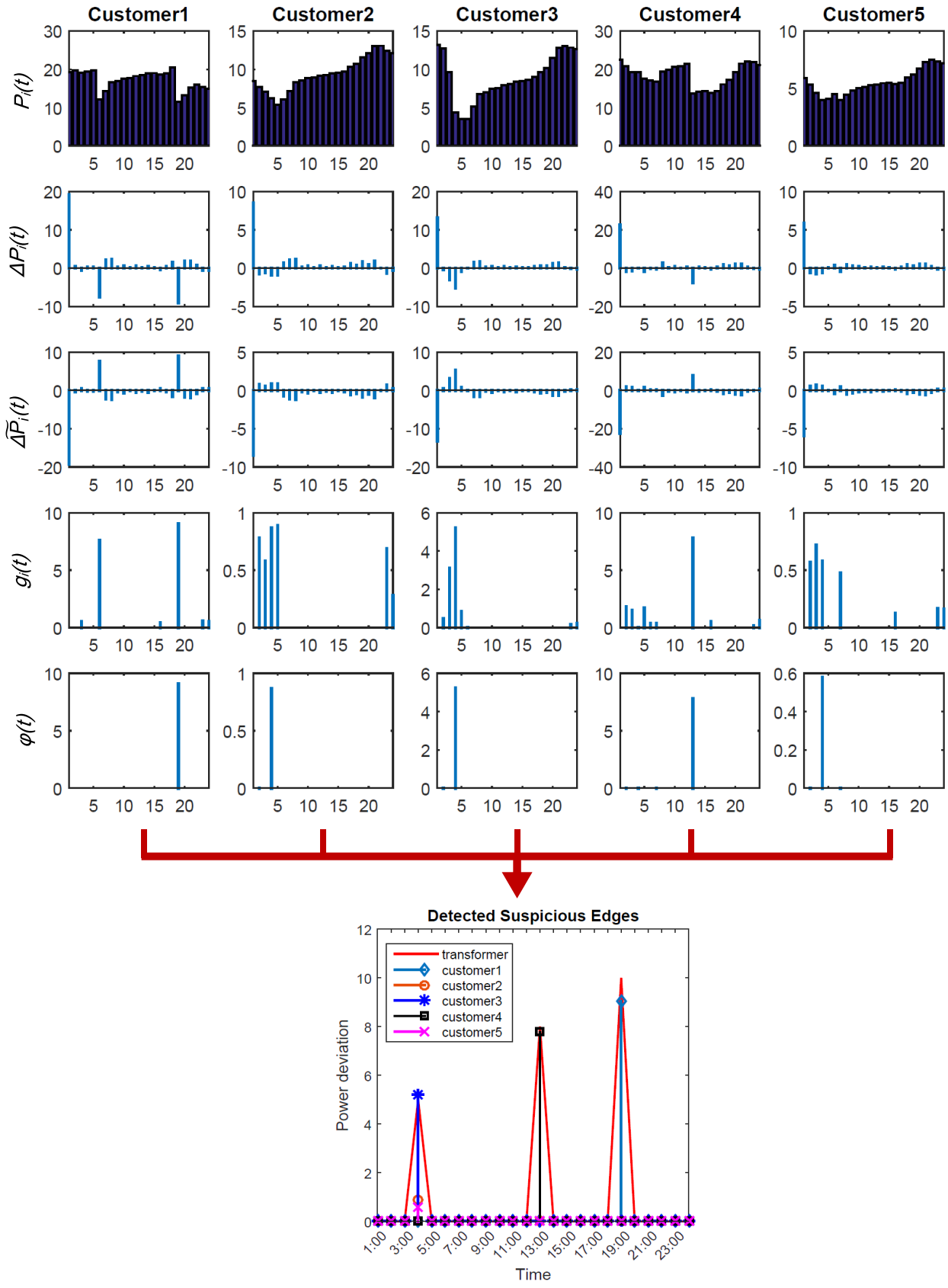

FIGURE 8. RTDI algorithm detection stages for five customers.

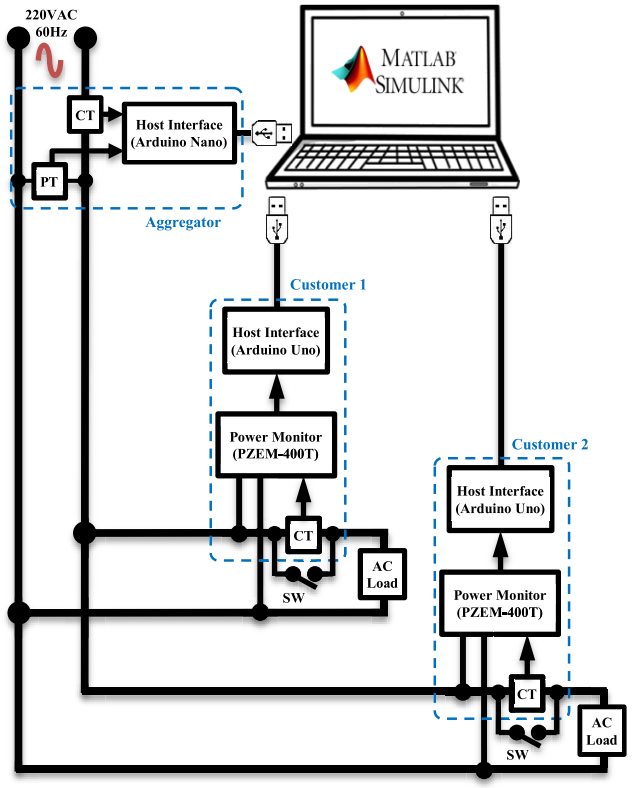

FIGURE 9. Block diagram of the experimental setup.

three hardware meters send the measured power values via their serial ports to a PC running a similar Simulink model to that used in the software simulation but with 5 meters and replacing the first two software meters (i.e. the meters of customer 1 and customer 2) with serial port blocks to receive the power consumption from the real-world meters. Thus, two of the five meters are real-time hardware meters and the other three are software meters. The aggregated power of the two hardware meters which is measure by the third central hardware meter and sent to the Simulink model is added to the aggregated power of the three software meters and the total sum of all the five meters is fed to the MIU block. Fig. 9 shows the block diagram of the HIL experimental setup.

Arduino Uno boards with LCD display and PZEM-400T single phase energy metering modules are utilized to build the energy meters for customer 1 and customer 2. Each meter is shunted by a switch to emulate electricity theft. The aggregator is built based on Arduino Nano, SCT-013 current transformer (CT), and ZMPT101B potential transformer (PT). The hardware experimental setup is shown in Fig. 10.

IV. RESULTS AND DISCUSSION

A. SOFTWARE SIMULATION RESULTS

This section presents the software simulation results obtained with the proposed scheme. The RTDI algorithm was verified by simulating three scenarios. In the first scenario, six

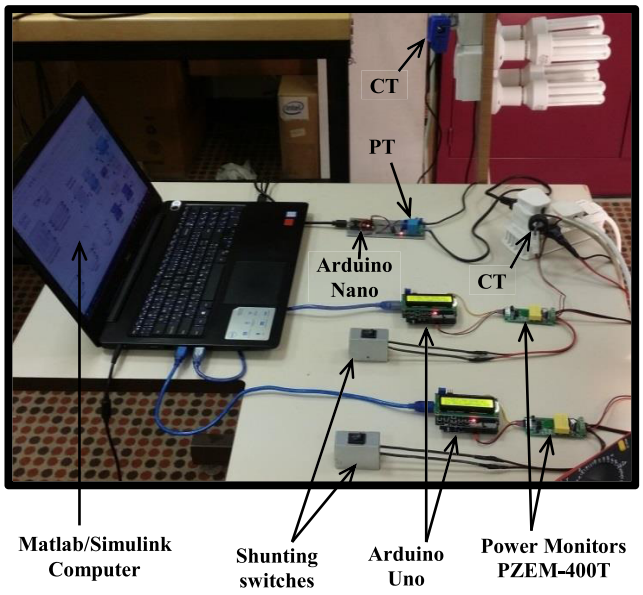

FIGURE 10. Experimental setup to validate the proposed algorithm.

customers out of ten were stealing electricity by tampering with their meters. The six customers started the tampering at different instants, which made it easy to detect each theft event individually. In the second scenario, three of the six tampering events started at the same instant of time to test the capability of the algorithm to detect simultaneous theft events. In the third scenario, two illegal users were stealing electricity by directly tapping the overhead feeder. The results of these three scenarios are presented and discussed in the following subsections.

1) SCENARIO I: INDEVEDUAL THEFT EVENTS

In this scenario, six electricity theft events that occurred at different instants during the day are simulated and the detection results of the proposed RTDI algorithm are shown in Fig. 11. It can be seen from Fig. 11 that the customers with the meters number 4, 3, 9, 1, 8 and 6 started electricity theft by tampering with their meters at the times 4:00 am, 5:00 am, 6:00 am, 8:00 am, 2:00 pm and 11:00 pm, respectively, and they are detected successfully.

2) SCENARIO II: SIMULTANEOUS THEFT EVENTS

In this scenario, six energy theft events were simulated and three of these events occurred at the same moment as can be seen in Fig. 12. Where the customers no. 1, 4 and 9 started the electricity theft at exactly the same time (7:00 am), whereas the customers no. 3, 5 and 8 separately started the theft at 4:00 am, 12:00 pm and 7:00 pm, respectively. The algorithm detected, in the real time, all of the theft events successfully.

3) SCENARIO III: FEEDER TAPPING THEFT

The tapping of overhead power feeder is one of the most common methods of electricity theft. It can be noticed from

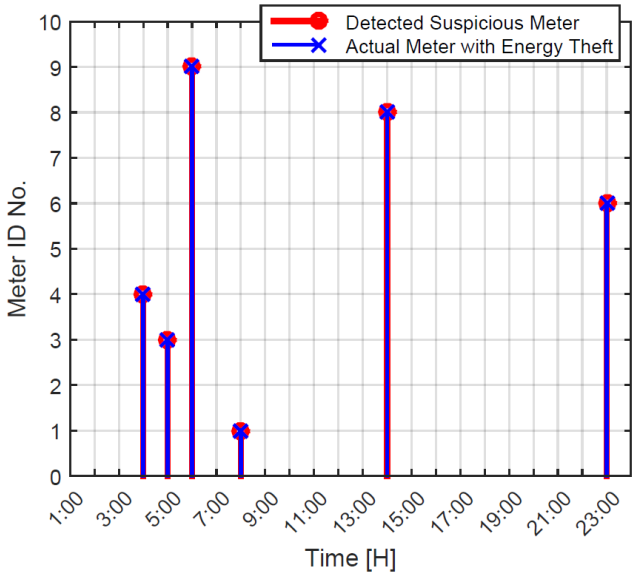

FIGURE 11. Separately occurred electricity theft events detected for six customers, namely, customers no. 1, 3, 4, 6, 8 and 9 at different instants.

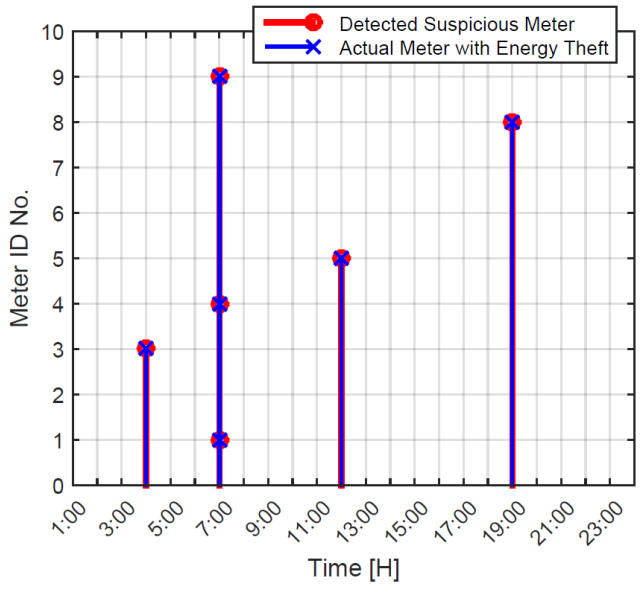

FIGURE 12. Simultaneously occurred electricity theft events detected for three customers, namely, customers no. 1, 4 and 9 with individual events for customer no. 3, 5 and 8.

Fig. 13 that two feeder tapping events occurred at different times. The first tapping occurred at 8:00 am and the second tapping occurred at 3:00 pm. In Fig. 14, two feeder tapping events occurred at the same instant of time (the probability of this to occur within the same T-Zone is very low), and the algorithm detected them as a single tapping event with a load equals to the sum of the two individual loads.

The simulation results in Fig. 13 and Fig. 14 show the effectiveness of the RTDI algorithm to detect the occurrence

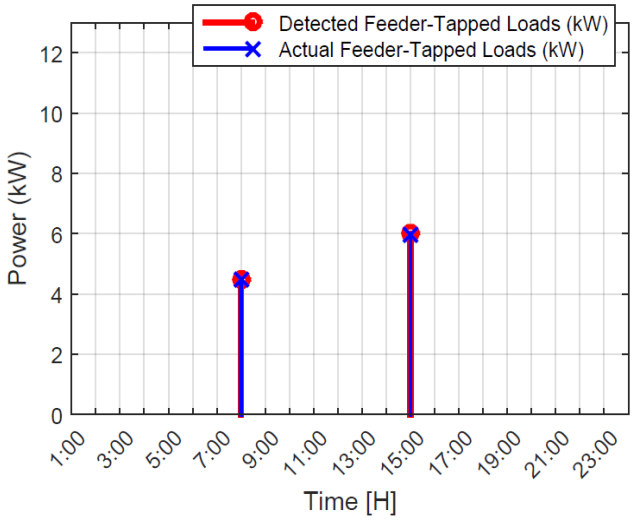

FIGURE 13. Two overhead feeder tapping detected at different instants.

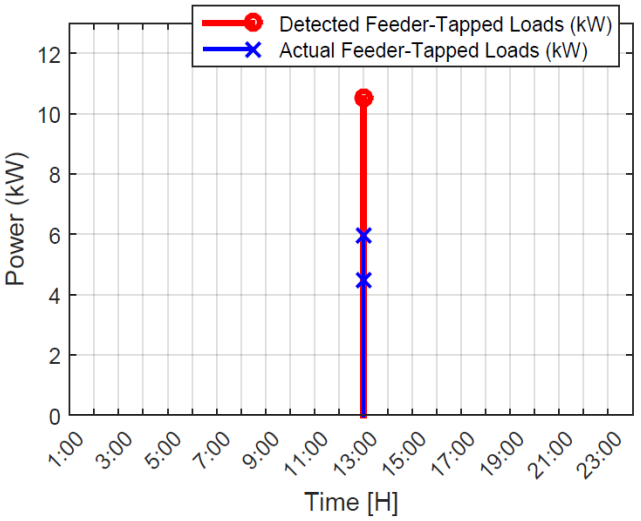

FIGURE 14. Two overhead feeder tapping detected at the same instant.

of feeder tapping. Although the algorithm cannot determine the tapping locations, it helps to determine whether the deviation between $P_T(t)$ and $\sum_{i=1}^{N} P_i(t)$ is due to meter tampering or feeder tapping. The tampered meters will be accurately identified by the algorithm. However, once illegal feeder-tapped loads with significant power consumption are detected, they can be either located by physical inspection of the distribution feeders within the T-Zone only (which contains a limited and usually small number of customers), or the MIU can destroy appliances of the illegal users within the T-Zone. This can be accomplished by adding a harmonic generator at the MIU as the one proposed in [1]. Once considerable feeder-tapped loads are detected by the RTDI algorithm, the MIU will send disconnection commands to all the meters within the T-zone and operate the harmonic generator to destroy any feeder tapped load while keeping the legal customers isolated from the harmonic generator signal.

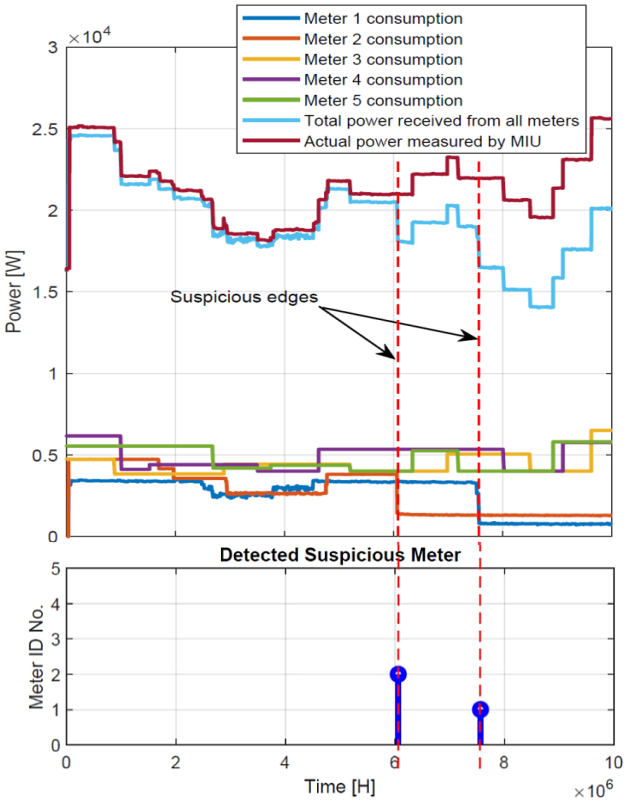

FIGURE 15. Two separately occurred electricity theft events detected for meter 1 and meter 2.

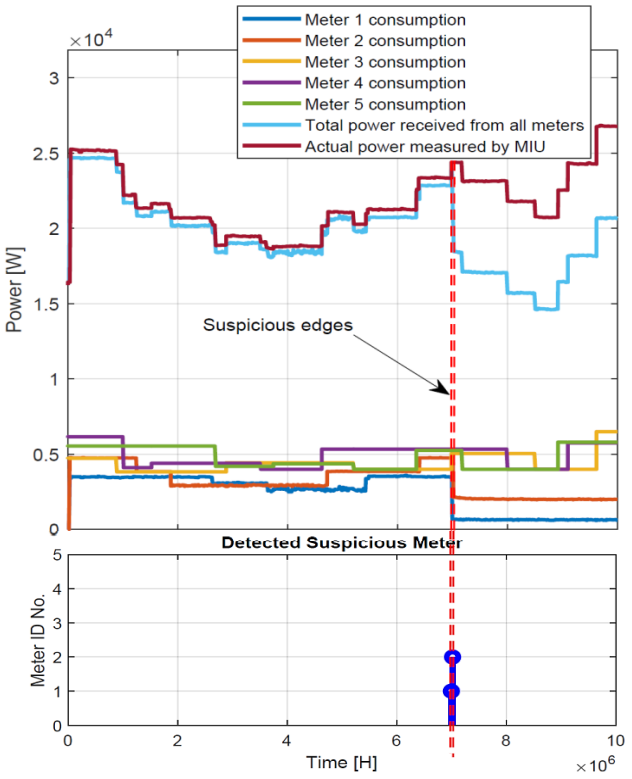

FIGURE 16. Two concurrently occurred electricity theft events detected for meter 1 and meter 2.

The method proposed in [1] can stop feeder-tapped loads but cannot detect tampered meters. Therefore, combining our proposed method with this method will help to stop both types of electricity theft.

B. HIL SIMULATION RESULTS

For further validation of the proposed algorithm, HIL simulation were conducted. As in the software simulation, three scenarios of electricity theft were considered. The results of these scenarios are presented and discussed in the following subsections.

1) SCENARIO I: SEPARATE THEFT EVENTS

In this scenario, the electricity theft occurred by the two hardware meters only. Meter 2 started the electricity theft by closing the shunting switch to bypass the meter, and after few minutes the shunting switch across meter 1 was closed to bypass the meter. Both of the theft events were detected efficiently by the algorithm as can be seen in Fig. 15. It can be noticed that only the falling edges in the power profiles of meter 1 and meter 2 are recognized as suspicious edges. Moreover, only the falling edges of meter 1 and meter 2 occurred at the time the significant deviation arose between total power received from all the five meters and the actual power drawn from the grid and measured by the MIU.

2) SCENARIO II: SIMULTANEOUS THEFT EVENTS

To examine the capability of the algorithm to detect simultaneous theft events by the hardware meters, the two shunting switches of meter 1 and meter 2 were closed simultaneously to start electricity theft in the same instant of time. Fig. 16 illustrates the effectiveness of the algorithm to detect both of the theft events in the real time. It can be noticed from Fig. 16 that although the suspicious edges are coinciding with each other, both of the suspicious meters are individually detected and identified.

3) SCENARIO III: FEEDER TAPPING THEFT

Detection of feeder tapping by the algorithm was also examined using HIL simulation. An AC load is connected before the two hardware meters and switched on during the HIL simulation. The algorithm detected the occurrence of feeder tapping. Moreover, the power consumption of this illegal load was determined too. Fig. 17 shows the detection result of this scenario. It can be noticed from Fig. 17 that the feeder-tapped load is detected at the instant at which a significant deviation occurred between the sum of the instantaneous power consumption of the five customers and the actual total power consumption measured by the MIU. The detected load is 1300 W, which is very close to the actual load we tapped to the line between the central meter and the two hardware meters.

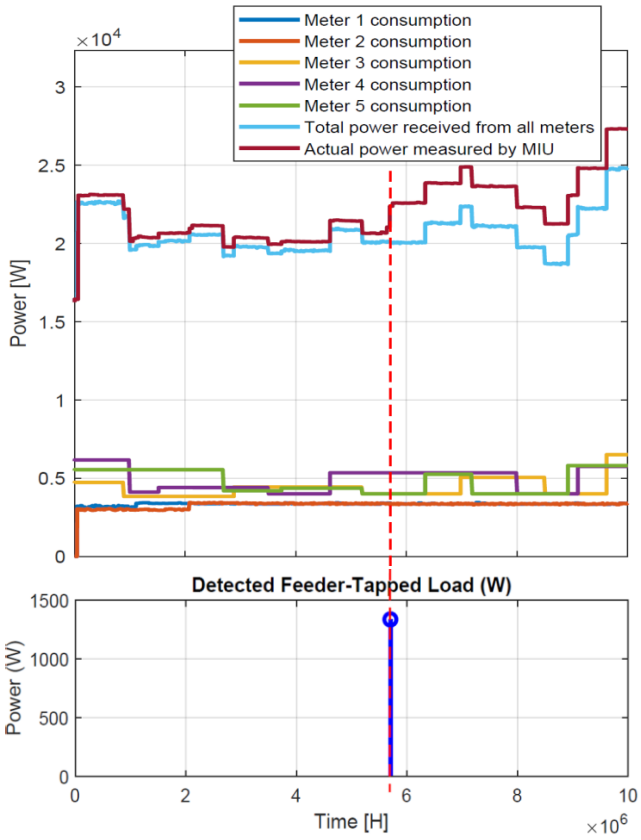

FIGURE 17. Detection of illegal feeder-tapped load of about 1300 W.

V. CONCLUSION

In this paper, we propose a cost-effective detection method that can remotely detect illegal electricity consumption and identify the illegal users in the real time without any pre-processing or extensive analysis of huge amount of collected data as in data-mining based methods. Furthermore, the proposed scheme can be applied on any existing AMR system with simple additions and modifications. Additionally, the scheme can be applied to prosumer installations. Where only the imported (consumed) power of prosumer will be sent to the MIU and not the net consumption. This means the prosumer will be treated as a conventional consumer.

Since the proposed algorithm needs monitoring instantaneous power consumption of customers as most of fraud detection algorithms do, it may pose a serious risk to the privacy of customers. To preserve customers' privacy, the proposed algorithm does not store the high-resolution instantaneous data, or send these data to utility operator. However, the running difference process at the MIU destroys the collected data during the processing and detection stage.

Software and HIL simulation experiments were conducted in this work. For each type of experiments, three scenarios of electricity theft were considered. These scenarios are: (1) separate theft events, (2) simultaneous theft events, and (3) feeder tapping theft. All of the theft events were successfully detected and recognized by the algorithm. The achieved experimental results demonstrate the effectiveness of the proposed real-time detection scheme.

REFERENCES

[1] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft," *Energy Policy*, vol. 39, pp. 1007–1015, Feb. 2011.

[2] T. B. Smith, "Electricity theft: A comparative analysis," *Energy Policy*, vol. 32, no. 18, pp. 2067–2076, Dec. 2004.

[3] J. L. Viegas, P. R. Esteves, and S. M. Vieira, "Clustering-based novelty detection for identification of non-technical losses," *Int. J. Elect. Power Energy Syst.*, vol. 101, pp. 301–310, Oct. 2018.

[4] J. V. Spirić, S. S. Stanković, and M. B. Dočić, "Identification of suspicious electricity customers," *Int. J. Electr. Power Energy Syst.*, vol. 95, pp. 635–643, Feb. 2018.

[5] E. W. S. Angelos, O. R. Saavedra, O. A. C. Cortés, and A. N. de Souza, "Detection and identification of abnormalities in customer consumptions in power distribution systems," *IEEE Trans. Power Del.*, vol. 26, no. 4, pp. 2436–2442, Oct. 2011.

[6] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni, and R. C. Green, "High performance computing for detection of electricity theft," *Int. J. Electr. Power Energy Syst.*, vol. 47, pp. 21–30, May 2013.

[7] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed, and M. Mohamad, "Nontechnical loss detection for metered customers in power utility using support vector machines," *IEEE Trans. Power Del.*, vol. 25, no. 2, pp. 1162–1171, Apr. 2010.

[8] R. Punmiya and S. Choe, "Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2326–2329, Mar. 2019.

[9] D. R. Pereira, M. A. Pazoti, L. A. M. Pereira, D. Rodrigues, C. O. Ramos, A. N. Souza, and J. P. Papa "Social-spider optimization-based support vector machines applied for energy theft detection," *Comput. Electr. Eng.*, vol. 49, pp. 25–38, Jan. 2016.

[10] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar, and S. Mishra, "Decision tree and SVM-based data analytics for theft detection in smart grid," *IEEE Trans. Ind. Informat.*, vol. 12, no. 3, pp. 1005–1016, Jun. 2016.

[11] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed, and F. Nagi, "Improving SVM-based nontechnical loss detection in power utility using the fuzzy inference system," *IEEE Trans. Power Del.*, vol. 26, no. 2, pp. 1284–1285, Apr. 2011.

[12] Z. Zheng, Y. Yang, X. Niu, H.-N. Dai, and Y. Zhou, "Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids," *IEEE Trans. Ind. Informat.*, vol. 14, no. 4, pp. 1606–1615, Apr. 2018.

[13] M. A. Uparela, R. D. Gonzalez, J. Jimenez, and C. G. Quintero, "Intelligent system for non-technical losses management in residential users of the electricity sector," *Ingeniería e Investigación*, vol. 38, no. 2, pp. 52–60, May/Aug. 2018.

[14] A. A. Ghasemi and M. Gitizadeh, "Detection of illegal consumers using pattern classification approach combined with Levenberg–Marquardt method in smart grid," *Int. J. Elect. Power Energy Syst.*, vol. 99, pp. 363–375, Jul. 2018.

[15] S.-C. Yip, K. Wong, W.-P. Hew, M.-T. Gan, R. C.-W. Phan, and S.-W. Tan, "Detection of energy theft and defective smart meters in smart grids using linear regression," *Int. J. Electr. Power Energy Syst.*, vol. 91, pp. 230–240, Oct. 2017.

[16] S.-C. Yip, W.-N. Tan, C. Tan, M.-T. Gan, and K. Wong, "An anomaly detection framework for identifying energy theft and defective meters in smart grids," *Int. J. Electr. Power Energy Syst.*, vol. 101, pp. 189–203, Oct. 2018.

[17] J. V. Spirić, S. S. Stanković, and M. B. Dočić, "Determining a set of suspicious electricity customers using statistical ACL Tukey's control charts method," *Int. J. Electr. Power Energy Syst.*, vol. 83, pp. 402–410, Dec. 2016.

[18] L. G. de O Silva, A. A. P. da Silva, and A. T. de Almeida-Filho, "Allocation of power-quality monitors using the P-median to identify nontechnical losses," *IEEE Trans. Power Del.*, vol. 31, no. 5, pp. 2242–2249, Oct. 2016.

[19] J. V. Spirić, S. S. Stanković, M. B. Dočić, and T. D. Popović, "Using the rough set theory to detect fraud committed by electricity customers," *Int. J. Electr. Power Energy Syst.*, vol. 62, pp. 727–734, Nov. 2014.

[20] F. Xiao and Q. Ai, "Electricity theft detection in smart grid using random matrix theory," *IET Gener., Transmiss. Distrib.*, vol. 12, no. 2, pp. 371–378, Jan. 2018.
[21] S. K. Singh, R. Bose, and A. Joshi, "Entropy-based electricity theft detection in AMI network," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 3, no. 2, pp. 99–105, Jun. 2018.
[22] Z. Ouyang, X. Sun, J. Chen, D. Yue, and T. Zhang, "Multi-view stacking ensemble for power consumption anomaly detection in the context of industrial Internet of Things," *IEEE Access*, vol. 6, pp. 9623–9631, 2018.
[23] P. Glauner, J. A. Meira, P. Valtchev, R. State, and F. Bettinger, "The challenge of non-technical loss detection using artificial intelligence: A survey," *Int. J. Comput. Intell. Syst.*, vol. 10, pp. 760–775, Feb. 2017.
[24] G. M. Messinis and N. D. Hatziargyriou, "Review of non-technical loss detection methods," *Electric Power Syst. Res.*, vol. 158, pp. 250–266, May 2018.
[25] T. Ahmad, H. Chen, J. Wang, and Y. Guo, "Review of various modeling techniques for the detection of electricity theft in smart grid environment," *Renew. Sustain. Energy Rev.*, vol. 82, pp. 2916–2933, Feb. 2018.
[26] J. L. Viegas, P. R. Esteves, R. Melício, V. M. F. Mendes, and S. M. Vieira, "Solutions for detection of non-technical losses in the electricity grid: A review," *Renew. Sustain. Energy Rev.*, vol. 80, pp. 1256–1268, Dec. 2017.
[27] A. Fragkioudaki, P. Cruz-Romero, A. Gómez-Expósito, J. Biscarri, M. J. de Tellechea, and Á. Arcos, "Detection of non-technical losses in smart distribution networks: A review," in *Trends in Practical Applications of Scalable Multi-Agent Systems, the PAAMS Collection*. Cham, Switzerland: Springer, 2016, pp. 43–54.
[28] I. H. Cavdar, "A solution to remote detection of illegal electricity usage via power line communications," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Jun. 2004, pp. 896–900.
[29] A. Pasdar and S. Mirzakuchaki, "A solution to remote detecting of illegal electricity usage based on smart metering," in *Proc. 2nd Int. Workshop Soft Comput. Appl.*, Aug. 2007, pp. 163–167.
[30] B. Bat-Erdene, S.-Y. Nam, and D.-H. Kim, "A novel remote detection method of illegal electricity usage based on smart resistance," in *Future Information Technology*. Berlin, Germany: Springer, 2011, pp. 214–223.
[31] B. Bat-Erdene, B. Lee, M.-Y. Kim, T. H. Ahn, and D. Kim, "Extended smart meters-based remote detection method for illegal electricity usage," *IET Gener., Transmiss. Distrib.*, vol. 7, no. 11, pp. 1332–1343, Nov. 2013.

AHMED BIN-HALABI (S'13) received the B.S. degree in electronics and communication engineering from Hadhramout University, Mukalla, Yemen, in 2003, and the M.S. degree in electrical engineering from King Saud University, Riyadh, Saudi Arabia, in 2013, where he is currently pursuing the Ph.D. degree in electrical engineering.

His current research interests include automation and control, photovoltaic power systems, artificial intelligence, demand-side management, and smart grids.

ADNAN NOUH received the B.Sc. degree from Alexandria University, Egypt, in 1966, and the M.Sc. and Ph.D. degrees from Carnegie Mellon University, Pittsburgh, USA, in 1970 and 1973, respectively, all in electrical engineering.

He is currently a Professor with the Electrical Engineering Department, King Saud University, Riyadh, Saudi Arabia. His research interests include control systems, signal processing, optimization, and advanced logic design.

MOHAMMAD ABOUELELA received the B.Sc. and M.Sc. degrees from Ain Shams University, Egypt, in 1978 and 1982, respectively, and the Ph.D. degree from Clude Bernard University, Lyon, France, in 1987, all in electrical engineering. He joined the Electrical Engineering Department, Faculty of Engineering, Ain Shams University, in 1978, as an Instructor, where he was an Assistant Professor, an Associate Professor, and a Full Professor, in 1987, 1994, and 2000, respectively. He is currently a Full Professor with King Saud University, Riyadh, Saudi Arabia. His research areas include PLL, frequency synthesizers, PV systems, computer interfacing, M2M, and embedded systems.