A Survey of Remote Detection Method for Illegal Electricity Usage

[1]Mandakh Oyun-Erdene, [2]Dong Han-Kim, [*3]Bat-Erdene Byambasuren
[1] *Department of Automation for Electrical System, Mongolian University of Science and Technology, Mongolia, mandakh1819@gmail.com*
[2] *Department of Electronics and Radio Engineering, Kyung Hee University, Republic of Korea, donghani@khu.ac.kr*
[3]*Department of Automation for Electrical System, Mongolian University of Science and Technology, Mongolia, baterdene@must.edu.mn*

Abstract

Detection of illegal electricity usage is the most important issue for power delivery companies. Therefore, there is a need to attend for detection methods of illegal electricity usage and their accuracy. This paper reviews remote detection methods for illegal electricity usage. Detection methods of illegal electricity usage are divided into statistical methods, which are based on the support vector machine, statistical variance, genetic algorithm and real time methods, which are based on signal processing, inspection robot and smart energy meters. Especially, remote detection methods by real time are considered in this paper. Simulation and experimental results of these remote detection methods show the possibility and the feasibility of detection for illegal electricity usage.

***Keywords**: Illegal electricity usage, Remote detection method, Inspection robot, Smart energy meter, Automatic Meter Reading*

1. Introduction

In modern society, we can not live without the use of energy, where the amount of consumption is steadily increasing. As this increasing, illegal electricity usage is stagnatly existed on the power delivery system. In recent years, many researchers put emphasis on the detection issue of illegal electricity usage and several research outcomes were developed in this field [1]. Detecting and localizing illegal electricity usage is the prominent problem for power delivery companies in many countries [2, 3].

Many kind of detection methods for illegal electricity usage are researched in recent years. Those methods are classified two parts. One part is detection methods based on statistical tools, which use measurement data of energy users in several days and years. Other part is remote detection methods by real time.

Detection methods based on statistical tools use support vector machine, statistical variance, genetic algorithm and so on [4-6]. In addition, detection methods based on mathematical approach are used [7]. Furthermore, detection methods based time domain reflectometer in main power cable. In order to detect a fault in power line as well as the location of illegal connection, many companies or countries use detection methods based on the time domain reflectometer in the power cable of consumer. It uses signal analyses of reflected wave [8].

However, remote detection methods by real time for illegal electricity usage are classified follows: based on smart meters, high frequency signal process, inspection robot and so on. But, some method uses disconnection conception of energy users [9]. In addition, remote detection method for illegal electricity usage based on current difference between two energy meters is used [10].

[*] Corresponding Author
Received: Mar. 29, 2014, Revised May. 1, Accepted: Jun. 25, 2014

Especially, this paper presents realtime remote detection methods for illegal electricity usage without disconnection of energy users. Further, localization of illegal electricity usage, mathematical models, and accuracy of detection system are importantly considered in these methods [11-13].

2. Remote Detection Method for Illegal Electricity Usage Based on Two Energy Meters

Illegal electricity usage can be detected by the current difference between two energy meters, which are installed on the start and end section of transmission branch. In October 2004, H. Cavdar suggested a new Automatic Meter Reading-based (AMR) method of detecting illegal electricity consumption [10].

He assumed that electricity could be used illegally in the following four ways: switching of energy cables at the meter box (Case 1), use of an external phase before the meter terminals (Case 2), use of a fixed magnet (Case 3), and use of mechanical objects (Case 4). Note that Case 3 and Case 4 of illegal electricity usage do not occur for digital energy meters. Those type illegal electricity usages only occur for mechanical energy meters.

H. Cavdar's basic method involves the use of two electrical meters: one on the user side and the other placed outside the user's residence. Any variation in measurements between two energy meters confirms illegal electricity usage. H. Cavdar's method can detect any illegal consumption of electricity between any two points when the energy meter and the main energy meter are installed. H. Cavdar's proposed system for the detection of illegal electricity usage is shown Figure 1. PLC signaling is only transmitted by low voltage transmission line that is 220V alternative current (AC) power lines. The system should be used to every low voltage distribution network.

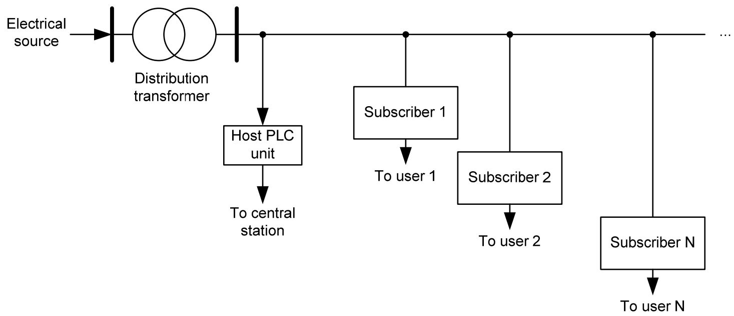

Figure 1. The proposed detection system of illegal electricity usage

Host PLC unit is placed in start point of second side of power transformer, which collects recorded data of energy meter that is placed on the every user and transmits collected data to central station. Every electrical user placed on this low voltage distribution network is connected by subscriber section. One subscriber includes two energy meters. Structure of one subscriber is shown in Figure 2.

Every subscriber consists of two PLC modems that are called PLC1A,…,PLCNA and PLC1B,…,PLCNB. For example, we can see k^{th} PLC modems of A and B from Figure 2.5. The addresses of those modems are k1 and k1.

The recorded data in energy meters for every subscriber are sent to host PLC modem via PLC modems which is placed in subscriber's locations. On the other hand, energy meter chips are located at the connection points and read the energy in energy meters and also send the data to host PLC unit. This proposed detector system has two recorded energy data in host PLC unit, one which comes from general energy meter that is installed by AMR system and the other which comes from the PLC modem at the connection points. These two recorded energy data are compared in the host PLC; if there is any difference between two readings, an error signal is generated. This means that there is an illegal usage in the network. After that, the subscriber address and error signal are combined and sent to the central control unit. In addition, there may be install a contactor to distribution network. In this condition, it can turn off the energy automatically, if there is an illegal usage in the network.

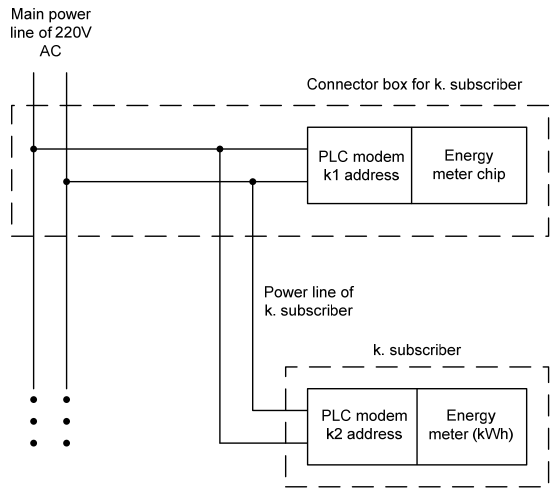

Figure 2. Detection system for one subscriber [10]

He carried out the tests of the proposed detection system in the laboratory, because the AMR system has not established a power grid in Turkey yet. Figure 3 shows system simulation and modeling of the detection system of illegal electricity usage.

However, in many countries, illegal consumption is rife through a street-level connection from the main power line without any energy meter. Thus, H. Cavdar's method requires extra numbers of energy meters and it can be only used on a single low voltage grid. The main disadvantage of this method is the usage of additional energy meter, which has to be installed on every transmission branch of users.

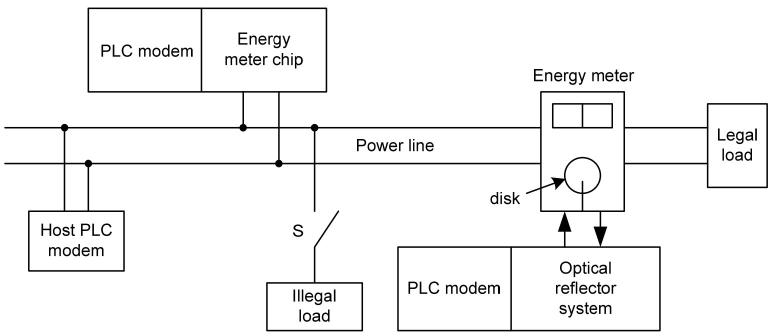

Figure 3. System simulation and modeling of the detection system for illegal electricity usage [10]

3. Line Impedance-based Method using High Frequency Signals

Illegal electricity usage can be detected by measuring the line impedance when the power delivery system of all users are disconnected and then a low voltage signal having high frequency component is transmitted to the power delivery system [9].

In 2007, A. Pasdar and S. Mirzakuchaki suggested that illegal electricity usage could be detected through on a smart meter-based a remote method. If smart meter is installed in power distribution network, the smart meter could disconnect all users to transmit a low voltage signal with high frequency through the main power line. Power line impedance is very little at 50 Hz. Therefore, high frequency signal is used, and an energy meter disconnection this sending has not any side effect. In this method, they used power line characteristic to determine the illegal node. Used low voltage power line characteristics are shown in Table 1. Furthermore, 2V signal with 150 kHz is used for grid characteristic recording. At 150 kHz signal the power line has good impedance per meter; the power line impedance at this frequency must be about 1 Ohm/m. Then, we can read different voltage at different node by analog digital converter of smart meter.

Table 1. Low voltage power line characteristic [9]

Reactance Ohm/km (50 Hz)	Resistance Ohm/km (+20°C)	Al/Fe, mm^2	Voltage (kV)
0.30	1.06	25.0	0.4
0.28	0.64	50.0	0.4
0.10	0.87	35.0	0.4

The method consists of following steps: when grid is installed, disconnect all load and main voltage from grid and send test signal to grid; record all node voltage and the main current; calculate impedance of each line and save those impedances by nodes name in the database; compare the parameters with normal operation; after detection of illegal usage, connect all loads. At this method, we need two kind of smart energy meter:

1. The energy meter that is installed at customer's home. This meter must has ability to disconnect the home's load from main voltage by receiving the disconnection command from server. Also, this smart meter must has ability two read the root mean square (RMS) voltage of test signal that it reads.
2. The smart meter that is installed at center transformer. This smart meter must has ability to generate test signal and disconnect grid from main voltage and send test signal to grid, this smart meter also must has ability to read the current that follow in grid when test signal is sent.

Their method detects illegal electricity usage by measuring and comparing the impedance value with that of a normal regime. However, the main drawback of their method is that all users of the power delivery system must be disconnected.

4. Detecting and Locating Method Based on High Frequency Signal Injection

In this research, an on-line method for detecting and locating a faulty node in the utility grid is proposed for smart grids. The method is based on injection of high frequency (A-Band) current signal into the grid that would impose voltages (less than 1V according to EN50065-1 standard) on the nodes to determine changes in the impedance characteristics. This detection is accomplished on-line without interrupting the power flow in the network [11].

In modern times, smart grid infrastructure can contribute towards power network automation which would improve the capabilities of existing power networks significantly. The power and information flow diagram of a smart grid network in the low voltage side (LV) is shown in Figure 4 where each individual smart meter communicates with the central unit. Two important elements in the smart grid network are the smart meter (SM) and the central unit.

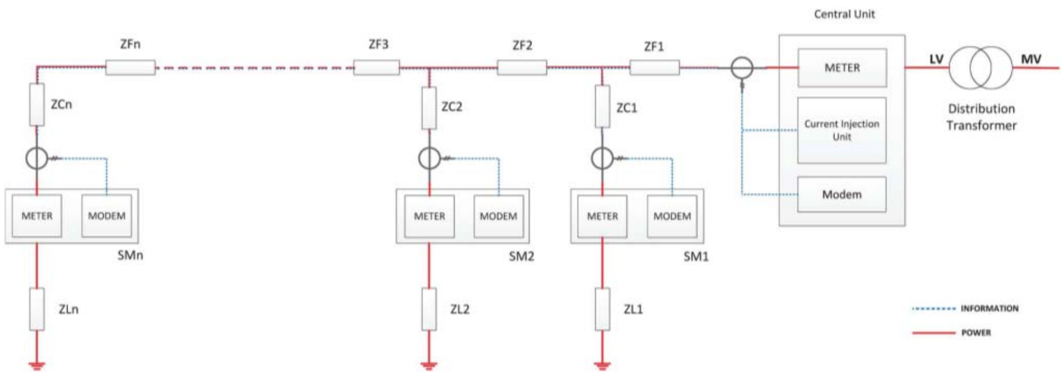

Figure 4. Power and information flow diagram [11]

The proposed method requires two units for proper operation. The first unit is a common smart meter that should measure the data needed to calculate the impedance characteristics of each node; this unit also has the ability to store data into external memory and send it to the host via a physical layer. The meter transducer should have wide bandwidth to measure the current and voltage of the received signal. Another unit is the modem which sends data to a specified node. The smart meter unit is based on commercial energy meter chips that have the ability to measure most of the energy usage parameters. Each meter sends six data to the host unit to calculate the impedance of the power line at low frequency. The power usage of each node is computed and transferred to the main unit.

In this research, a constant amount of current is injected into the network to determine the difference between the predicted and measured power line impedance model. A programmable current source is used for this purpose. The proposed current injection unit is considered to be installed in the central unit. A constant value of the current is injected to maintain the limitation set by the standard, the maximum peak-to-peak imposed voltage is 120 dB (μV) which is equal to 1 V.

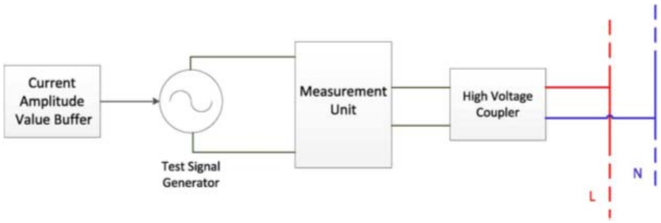

Figure 5. Test signal injection unit [11]

One of most important data needed for detecting and localizing the place of the faulty node (FN) is the power line network impedance model which consists of the node's load impedance model and each feeder segment's impedance model. Reactive as well as active power measured at each node determines the basic version of the node load impedance at low frequency. The real and imaginary parts of the impedance are determined separately. The characteristics of these two elements are determined based on the apparent power as well as active power which are measured by the smart meters. The impedance of the power line frequency is converted to the current injection level at high frequency.

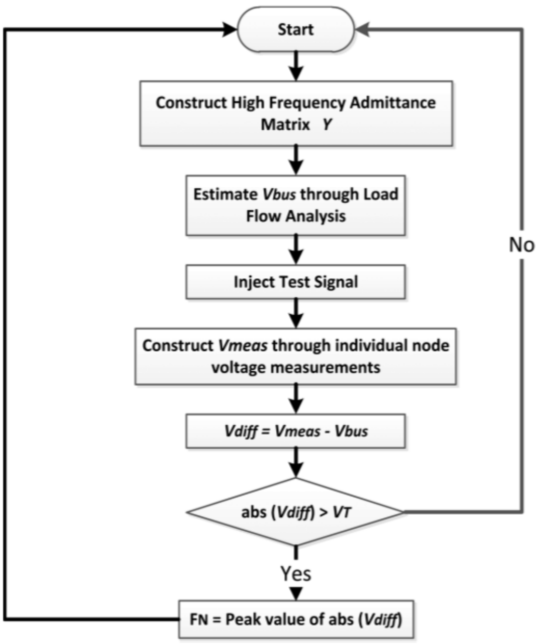

Figure 6. Detecting and localizing the FN procedure flow diagram [11]

The flow diagram for the detection and localization method is given in Figure 6.The array of the node voltages based on simulation of a predefined model with respect to test signal injection is Vbus. The array of the measured high frequency received signal voltage at the nodes due to the injection of the test signal in the real world is Vmeas. The detection unit runs the specific procedure at each iteration based on the two input matrices to detect the existence of the FN on the network. The difference between the measured and estimated voltage arrays is given as:

$$\text{Vdiff} = \text{Vmeas} - \text{Vbus} \qquad (1)$$

In the absence of a FN, Vdiff will be null. Vdiff is used to show the changes in the predefined network impedance model. Each element in the array is compared with the threshold value.

5. Energy Theft Detection in Smart Grids Based on Honesty Coefficient

Illegal usage can be indicated by honesty coefficient k_j of user's that computed by using Linear System of Equations (LSE).In particular, two distributed privacy-preserving energy theft detection algorithms based on Lower and Upper triangular matrix (LU) decomposition, called LUD and with partial pivoting decomposition (LUPD), respectively, which can identify fraudulent users without invading any user's privacy. Moreover, the LUD and LUDP algorithms are proposed in the case that users commit energy theft at a constant rate, i.e., with constant honesty [14].

In this research, to solve in a distributed fashion a linear system of equations privacy preserving illegal energy usage detection algorithm proposed. First of all, researchers assume that possible attacks on smart meters (SMs) by illegal users, and possible implementations of the proposed algorithms on the SMs. SMs can provide the users with a plethora of unique features. However, compared to mechanical meters which can only be physically tampered, smart meters are vulnerable to more types of attacks, which may make energy theft easier to commit and hence an even more serious problem in smart grids. The proposed algorithms can address all these problems.

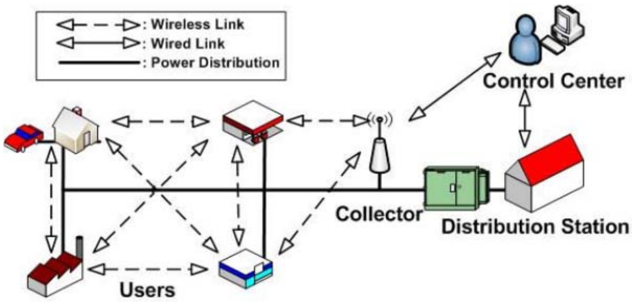

Figure 7. A typical architecture of Neighborhood Area Network (NAN) [14]

Typical network architecture is depicted in Figure 7. In a serviced area, the users' SMs together with the collector form a Neighborhood Area Network (NAN).The communications between SMs and the collector are carried out wirelessly due to SMs' communication capability, while the communications among the control center, the distribution station, and the collector are conducted via wired medium.

This work proposed to solve in a distributed fashion a Linear System of Equations (LSE), which involves the respective energy consumption of n users in a neighborhood at n time instances and the total energy consumption of the n users measured at a local data collector, for the user's "honesty coefficients". If a user's honesty coefficient is equal to 1, this user is honest. Otherwise, if the honesty coefficient is larger than 1, then this user has reported less consumed energy. Hence, this user is committing illegal electricity usage.

Consider a neighborhood of n users. We define a sampling period denoted by SP. Then, after every sampling period, all the $n + 1$ SMs will record their energy consumption in the past sampling period. We denote such energy consumption recorded by user j ($1 \leq j \leq n$) and by the collector at time t_j, by $\rho_{ti,j}$, and $\bar{\mathcal{P}}_{t_i}$, respectively. We further define an honesty coefficient, denoted by k_j where $k_j > 0$, for each user j. Thus,$k_j \cdot \rho_{t_{i,}j}$ gives the real energy consumption by user j from time instant $t_i - SP$ to time instantt_i. Since the sum of all the recorded energy consumption at time t_i must be equal to the total energy consumption of the neighborhood measured at the collector at time t_i, we have

$$k_1 p_{t_{i,}1} + k_2 p_{t_{i,}2} + \cdots + k_n p_{t_{i,}n} = \bar{\mathcal{P}}_{t_i} \qquad (2)$$

Our objective is to find all the k_j's. Obviously, 1) if $k_j = 1$, then user j is honest and did not steal energy; 2) if $k_j > 1$, then user j recorded less energy than what he/she consumes and hence is an energy thief; and 3) if $0 < k_j < 1$, then user j recorded more than what he/she consumes, which means that smart meter may be malfunctioning. In order to solve fork_j's, it needs$n$ independent linear equations like the one shown above. With n linear equations, it can thus have a linear system of equations as follows:

$$k_1 p_{t_1,1} + k_2 p_{t_1,2} + \cdots + k_n p_{t_1,n} = \bar{\mathcal{P}}_{t_1}$$
$$\vdots$$
$$k_1 p_{t_n,1} + k_2 p_{t_n,2} + \cdots + k_n p_{t_n,n} = \bar{\mathcal{P}}_{t_n}$$

This LSE can also be formulated in matrix form:

$$\boldsymbol{Pk} = \bar{\boldsymbol{\mathcal{P}}} \quad (3)$$

The j^{th} column of $\boldsymbol{P}$ represents the data recorded and stored by user j or SM_j, while the i^{th} row of $\boldsymbol{P}$ represents the data recorded by all the users at t_i. Besides, finding the honesty coefficient vector, $\boldsymbol{k}$, is delay tolerant. In other words, $\boldsymbol{k}$, is not required to be found and transmitted to the collector in real time. This gives priority to other real time traffic in the NAN, such as electricity pricing, incentive-based load reduction signals, and emergency load reduction signals.

Disadvantage of this method, at each of the serviced areas, the collector is placed. Besides SMs installed at each consumers, one SM is required at each collector to measure the total energy consumed by the serviced area.

6. Extended Smart Meters-based Remote Detection Method

In the proposed method for illegal electricity usage, two extended smart meters - terminal smart meter (TSM) and gateway smart meter (GSM) - are used. TSM is installed on every user side, where GSM is installed on the nodes, as shown in Figure 8 [12].

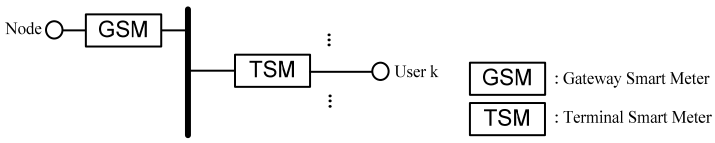

Figure 8. Detection system for illegal electricity usage using proposed two smart meters [12]

Since GSM is installed on the starting section of the node, it can connect and disconnect the node on the user side. The roles of TSM are to detect and measure illegal electricity usage. Block diagrams of GSM and TSM are shown in Figure 8.

If an illegal electricity usage does not exist on this node and there is normal, the following formula is valid:

$$E_{\text{node m}} = E_{\text{user 1 of node m}} + E_{\text{user 2 of node m}} + \ldots + E_{\text{user n of node m}} + E_{\text{lost}} \quad (4)$$

Where: $E_{\text{node m}}$ is energy value of GSM of the m^{th} node; $E_{\text{user 1 of node m}}$, $E_{\text{user 2 of node m}}$,…, $E_{\text{user n of node m}}$ are energy values on the TSM of each user's for the m^{th} node; E_{lost} is the energy lost and including the energy lost on the line of this node.

However, when an illegal electricity usage exists on a user of this node, above formula is not valid and not balanced. In this case, the remote detection system starts the detection process of illegal electricity usage from this node. On the other hand, the remote detection system attends to this node.

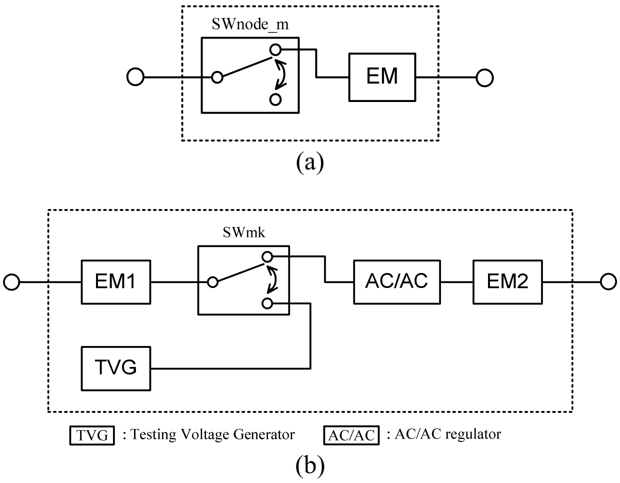

Figure 9. Block diagrams of proposed two extended smart meters. (a) Gateway smart meter (GSM), (b) Terminal smart meter (TSM) [12]

In order to detect the illegal electricity usage, the process of the proposed detection method includes two cases. The first case is to check whether a shunt connection exists on the current coil of the energy meter by using TSM. The illegal way of either mechanical locking or magnetic disturbance cannot occur in this case because a digital energy meter is used. The second case is to check whether an electrical energy exists from the phase of energy meter on the TSM of each user.

The proposed detection method checks for illegal electricity usage on the node of each user because it could exist in any node of the power delivery system on the user side. TSM is used to check this type of illegal electricity usage, where an AC/AC regulator and EM2 energy meter are used as well as the input switch SWmk as shown in Figure 9 (b). In order to check for shunt connections, the proposed detection method changes the input voltage of the energy meter to a low value by using an AC/AC regulator. After this, EM2 measures the variation in output voltage.

If there is no shunt connection, the output voltage is switched to low amplitude for a short period of time, and then returned to the previous normal value according to the control command given from processing control block using the AC/AC regulator. In contrast, the output voltage cannot be controlled according to the control command if the energy meter has shunt connections. In this case, there is no variation on the output voltage and its value would equal to the input voltage.

When a shunt resistance is connected, the shunt resistance is approximately equal to zero. The resistance of the AC/AC regulator is greater than the shunt resistance. Thus, the current is passed to the branch with minimum resistance according to Ohm's law. This way, the output voltage does not change according to the control command of the AC/AC regulator in TSM and illegal electricity usage can be detected.

However, the proposed detection method checks for an illegal branched connection of the energy meter. In this case, GSM, EM1, SWmk, testing voltage generator (TVG), AC/AC regulator and EM2 of TSM shown Figure 9 (b) are used.

In order to detect branched connection, the switch SWmk of TSM installed on the node of each user and the switch SWnode_m of GSM installed on the starting section of the node must be instantly and repetitively connected and disconnected at the same time for a very short period. Normal voltage is provided to the nodes on the user side by using an AC/AC regulator of TSM during repetition period. Then, the proposed detection method checks for illegal electricity usage of each user by using TSM.

As an example, consider the k^{th} user of the m^{th} node. In order to check for illegal electricity usage on the outside phase of the user k, proposed detection method uses TVG with the low voltage source with a high-frequency in the TSM. The low voltage source with a high-frequency is connected through the switch SWmk when the switch SWnode_m of GSM is disconnected.

If SWnode_m is connected and SWmk is connected to an AC/AC regulator, the signal is sinusoidal with the low frequency. However, if SWnode_m is disconnected and SWmk is connected to TVG, the signal is also sinusoidal, but its amplitude is low and frequency is high.

The GSM measures the important parameters when SWmk is connected to TVG. In this case, the impedance of Line k between the starting section of the node and the user k can be calculated by using the measured parameters. If the line has no illegal connection, the calculated impedance should equal to the original impedance of the line. However, if it has an illegal connection, the calculated impedance will be different compared to the original impedance of the line. In order to detect illegal electricity usage for all users, this operation should be executed for each user in order.

So, there is possible to detect an illegal electricity usage in the all users of the node according to the mentioned two algorithms.

7. Detection and Localization of Illegal Electricity Usage Based on Inspection Robot

Sometimes, illegal electricity usage on the power delivery system may be occurring on a low-voltage air transmission line. In this method, a novel method is proposed to detect and to define the location of illegal electricity usage on an air transmission line. The proposed method measures the current value of illegal electricity usage under the transmission line by using an inspection robot. Once the illegal current value is calculated, then it can define the location of illegal electricity usage. The proposed method does not require the installation of additional energy meters on the transmission branch of end-consumers. Significantly, the proposed method can detect illegal electricity usage in real-time without disconnecting the end user's electric connection.This research presents a new trend ofinspection robots for use in a smart grid system, as well as, robot navigation using air electrical transmission line.Furthermore, the proposed method can be extended to detect the fault location for power distribution systems [13].

They assume that energy distribution system has infrastructure as shown Figure 10 (a).

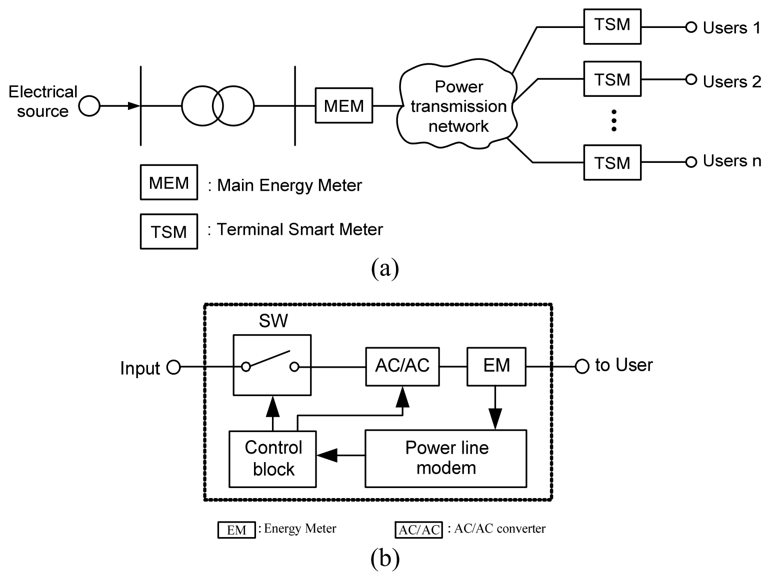

Figure 10. Structures: (a) proposed power delivery system, (b) terminal smart meter [13]

As shown in Figure 10 (a), the main energy meter (MEM) and terminal smart meter (TSM) are installed on the starting node and on the final end of each electrical user, respectively. MEM measures the total energy of all electrical users, whereas TSM measures the energy usage of each user and transmits the measured value through a power line, when there is no illegal electricity usage. If an illegal electricity usage occurs on the power delivery system, the measured value of MEM and the summation of each TSM measurements will not be equivalent. In this case, the proposed method begins the detection process by switching the status of TSM's. Note that the switches of a TSM can be either turned on or off simultaneously by the command of control block with a high frequency component.

The structure of a TSM is shown in Figure 10 (b). Voltage sag is converted to a normal voltage by AC/AC converter, which is created by the switching frequency. Then, the normal voltage is delivered to an electrical user, while the energy meter can measure user voltage, as a normal condition. In this case, the main current is measured by the MEM, which only expresses illegal electricity current when user's currents are switched off by TSM's.However, when a user's currentis switched on by a TSM, the measured current of the MEM represents the total current of the power distribution system.In the proposed method, the inspection robot is used to measure the current of a power transmission line. The inspection robot can propagate under the transmission line and detect obstacles using a charge-coupled device (CCD) camera and other sensors. When the robot detects an obstacle, it can pass through by the obstacle. In this research, the inspection robot will sense an illegal currenttap by a remote current sensor, which is filtered from the measured line current when user's currents are switched off by TSM's.

To detect and localize of illegal electricity usage, the illegal current should be separated from measured current using the inspection robot. Figure 11 shows the signal process to separate the illegal current.

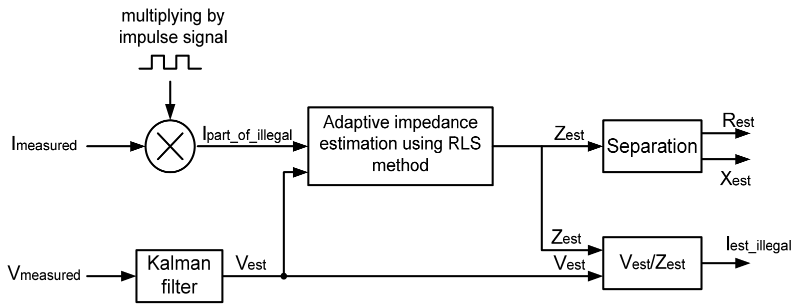

Figure 11. Separation process of illegal current [13]

When the measured current from the inspection robot is multiplied by an impulse signal, the illegal current section can be extracted. In this case, the impulse signal becomes active when users are disconnected by TSMs. In addition, the measured current can be multiplied by another active impulse signal when users are connected by TSMs. In this condition, multiplied current represents the total component of current.

Furthermore, the measured voltage from the power delivery system is filtered by a Kalman filter (KF) from the noise of measurement equipment. Because a KF generates efficiency response for sinusoid signals with constant frequency. After that, the adaptive impedance is estimated by values of multiplied illegal current section and filtered voltage using Recursive Least Square (RLS) method.

However, the multiplied values of extracted illegal current will be equal to zero when the impulse signal is inactive, which is called the focusing section. In the focusing section, original illegal current values will disappear. Therefore, an estimation of original illegal current values is necessary in the focusing section. For estimation, the impedance values of illegal electricity usage should be calculated using measured current and filtered voltage when impulse signal is active. It is assumed that illegal electricity usage is not changed and is constant. Then, calculation of the illegal current is possible using an estimated impedance and filtered voltage. Now, calculation of impedance is possible using the RLS method. After the calculation of impedance, illegal current can be plotted by estimated impedance and filtered voltage. In addition, resistance and reactance can be defined from estimated impedance.

8. Conclusion

This paper reviewed remote detection methods for illegal electricity usage. The reviewed papers, they presents remote detection methods for illegal electricity usage based on smart meters, extended smart meters, signal processing, and inspection robot. They also show mathematical models, experimental and simulation results of various type solutions for illegal electricity usage.

9. References

[1] Bat-Erdene, B., Sang-Yep, N. and Dong-Han, K, "A novel remote detection method of illegal electricity usage based on smart resistance," *Future Information Technology, Communication in Computer and Information Science,* vol. 185, pp. 214-223, June. 2011.

[2] Smith, T. B, "Electricity theft – comparative analysis", *Energy Policy*, vol. 32, pp. 2067-2076, December. 2004.

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

[4] Nagi, J., Yap, K. S. and Tiong, S. K, "Non-technical loss analysis for detection of electricity theft using support vector machines," in Proc. of the IEEE Int. Conf. Power and Energy, 2008, pp. 907-912.

[5] Nagi, J., Yap, K. S.and Tiong, S. K, "Nontechnical loss detection for metered customers in power utility using support vector machines," *IEEE Trans. Power Delivery*, vol. 25, no. 2, pp. 1162-1171, April. 2010.

[6] Pok, H. L., Yap, K. S., Abidin, I. Z., Hashim, A. H., Hussien, Z. F. and Mohamad, A.M, "Abnormalities and fraud electric meter detection using hybrid support vector machine and modified genetic algorithm," in Proc. of the Int. Conf. on Electricity Distribution, Vienna, 2007, pp. 1-4.

[7] Bandim, C. J., Alves, J. E. R., Pinto, A. V., Souza, F. C., Loureira, M. R. B., Magalhaes C. A. and Galvez-Durand, F, "Identification of energy theft and tempered meters using central observer meter: A mathematical approach," *Transmission and Distribution Conference and Exposition, IEEE PES*, 2003, pp. 163-168.

[8] Trupinic, K., Stojkov, M. and Poleto, D, "Reduction of non-technical losses based on time domain reflectometer (TDR) principles and function," in Proc. of the Int. Conf. Electricity Distribution, Turin, 2005, pp. 1-5.

[9] Pasdar, A. and Mirzakuchaki, S, "A solution to remote detecting of illegal electricity usage based on smart metering," in Proc. of the IEEE Int. Workshop on Soft Computing Applications, 2007, pp. 163-167.

[10] Cavdar, H, "A solution to remote detection of illegal electricity usage via power line communications," *IEEE Trans. Power Delivery*, vol. 19, no. 4, pp. 1663-1667, June. 2004.

[11] Pasdar, A. M., Sozer, Y. and Husain, I, "Detecting and Locating Faulty Nodes in Smart Grids Based on High Frequency Signal Injection," *IEEE Transactions on Smart Grid*, Vol. 4, No. 2, pp. 1067-1075, June. 2013.

[12] Bat-Erdene, B., Bumjoo, L., Min-Young, K., Tae Hong, A. and Donghan, K, "Extended smart meters-based remote detection method for illegal electricity usage," *IET Generation, Transmission & Distribution*, Vol. 7, Iss. 11, pp. 1332-1343, November. 2013.

[13] Mandakh, O., Bat-Erdene, B., Matson, E. T. and Donghan, K, "Detection and Localization of illegal electricity usage in power distribution line," *Multimedia Tools and Applications*, Vol. 71, DOI: 10.1007/s11042-014-2022-2, May. 2014.

[14] Salinas, S., Ming, L. and Pan, L, "Privacy-Preserving Energy Theft Detection in Smart Grids," in Proc. of the Annual IEEE Communications Society Conference on Sensor, 2012, pp. 605-613.