ELECTRICITY THEFT DETECTION AND LOCALISATION IN UNKNOWN RADIAL LOW VOLTAGE NETWORK

Heman Shamachurn[1], Perenjordee Poollay Auroomoogum[2]

[1]*Lecturer, Electrical and Electronic Engineering, University of Mauritius, Reduit, Mauritius*
[2]*Undergraduate Student, Electrical and Electronic Engineering, University of Mauritius, Reduit, Mauritius*

Abstract

The distribution of electricity involves both technical and non-technical losses. One major cause of non-technical loss is the illegal abstraction of electricity which is also known as 'Electricity Theft'. The illegal usage of electricity has many associated problems, both for utilities and consumers of electricity, implying that there is a pressing need for theft detection and localisation. Traditional methods of identifying illegal electricity consumers are time consuming and ineffective as measurements have to be performed at a large number of suspected locations. Smart metering in future electricity networks will lead to a more efficient automated system for the detection and localisation of electricity theft. This will enable immediate action to be taken by distribution network operators against the offenders and will help to improve the quality, reliability and security of electricity supply systems. The aim of this study was to analyse the performance of an electricity theft detection and localisation technique in an unknown grid. The method assumed the availability of measured voltages, currents, and powers from installed smart meters. The detection step was a power comparison process and the localisation step was a voltage comparison process. The investigation involved analysis in the presence of single and simultaneous multiple thefts. To better represent future networks with increasing penetration of renewable energy generators, distributed generation was added to the system and the capability of the detection and localisation technique was further explored. All the simulations were performed in Matlab/Simulink. It was found that the method performed satisfactorily, with a minimum stolen power of 450 W successfully detected and localised.

Keywords: *Electricity Theft, Smart Meters, Double Feeding, Low Voltage Radial Network, Matlab/Simulink*

--***---

1. INTRODUCTION

Significant operational losses are involved in the generation, transmission and distribution of electricity. The losses can be classified as technical and non-technical. The technical losses are associated with the components of the power system and the non-technical losses (NTL) are associated with external factors which do not directly involve the power system. In some countries the illegal abstraction of electricity takes a major proportion of the NTL. For instance, 1200 GWh of electrical energy is illegally consumed from the distribution grid each year in the Netherlands, representing about 1% of the annual electricity generation [1]. Electricity theft is a main concern for utilities as the percentage of theft might be small overall, but the associated financial loss is significant [2].

Several methods are employed to steal electricity including tampering with the energy meter, bypassing the meter through double feeding and evading bill payments. Electricity theft can overload generator units as distribution network operators (DNOs) cannot forecast the illegal consumption, and if significant, the electricity supply can be interrupted due to demand-supply mismatch. Moreover, the stolen electricity increases grid losses and represents huge monetary losses both for the DNOs and the Government. Losses are eventually reflected in the price of electricity, which implies that genuine customers have a pay a higher electricity price because of illegal consumers [3].

Currently, tampering attempts are mostly detected by measurements of electrical parameters in suspected locations followed by an analysis of the acquired data. The whole process is time consuming and ineffective, especially in densely populated areas where there are many houses very close together and many branches in the distribution network. Smart meters and state of the art measurement systems in the future grid will make electricity theft harder [4]. The installed secure meters at the consumers' premises and in the substations will enable automated, fast and successful electricity theft detection and localisation while preventing tampering with the meter itself.

2. METHOD DESCRIPTION

2.1 Investigated Network Configuration

A three-phase, four-wire radial distribution system with a TT earthing arrangement for residential customers was considered. The model comprised a substation represented by a 11 kV/ 400 V three-phase transformer and 35 single-phase household loads as shown in Fig-1. The corresponding parameters are provided in Table-1. The distance between the substation and the first connected house downstream was 100 m.

Each house was represented as a single-phase load consuming both real and reactive powers. Each load was modeled by voltage and power controlled current sources [5]. The following assumptions were considered:

- Each house was connected to the network via a smart meter which could record the RMS voltage, the RMS current, the real and reactive power flows.
- The same measurement capabilities were present at the substation.
- The active power consumption of each house had a normal distribution with a mean and a variance of 1 kW.
- The reactive power consumption of each house had a normal distribution with a mean of 0 VAr and a variance of 200 VAr.
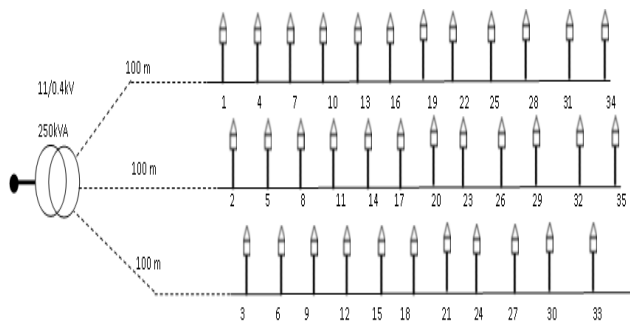

Fig-1: Simulated network

Electricity theft at a house was simulated by the connection of an illegal load in parallel to the house, but bypassing the smart meter as shown in Fig-2.
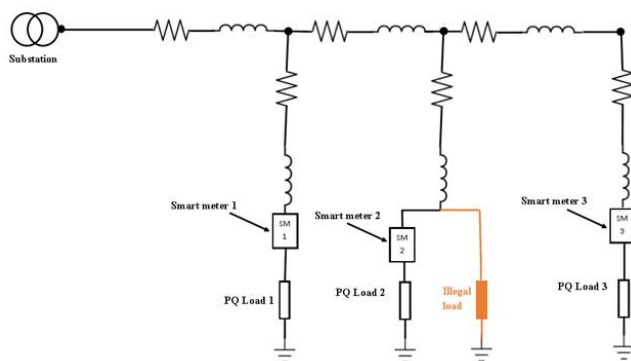
Fig-2: Illegal load connection

Table-1: Network parameters

Properties	Value
Average length between houses	9 m
Cross section of feeder sections	150 mm^2
Resistance of feeder	0.206 Ω/km
Inductance of feeder	0.318 mH/km
Length of connection cable between house and feeder	5 m
Cross section of connection cables	10 mm^2
Resistance of connection cable	1.83 Ω/km
Inductance of connection cable	0.402 mH/km

2.2 Electricity Theft Detection and Localization

During a given time step of the simulation, a probable electricity pilfering attempt was identified by a large difference between the total active power consumptions of all customers and the total active power measured at the substation, taking into account the technical losses throughout the feeder.

If a theft was detected, the localisation process would involve comparing the estimated grid voltage at each house to the actual measured voltage.

The following assumptions were made:
- Order of each house on the feeder was known
- Cable impedances were unknown
- Phase of each house was unknown

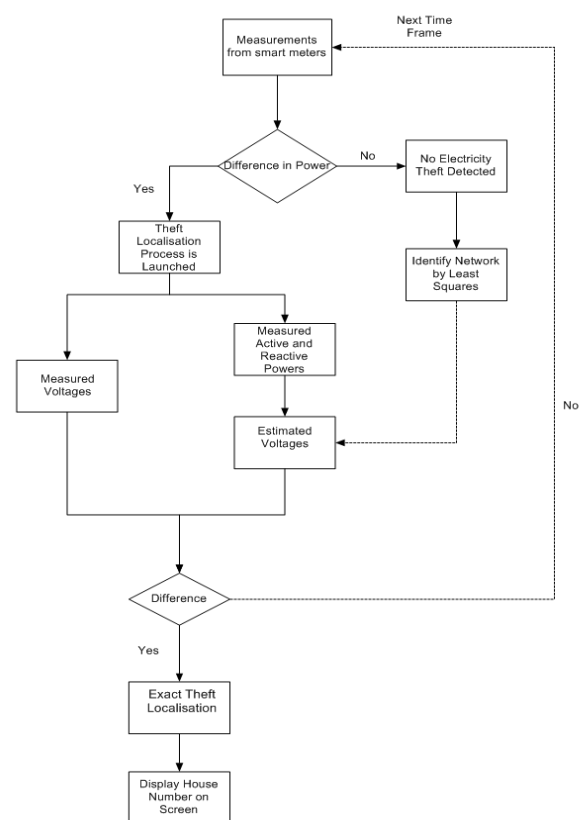The detection and localisation process is summarized in Fig-3 [6].

Fig-3: Theft detection and localisation for unknown grid

The non linear load flow problem [6] can be approximated by a linear model to obtain equation (1) where $V_{h,k}$ is the voltage at house h at time step k; V_k^0 is the voltage magnitude at the distribution transformer for the corresponding phase at time step k; $P_{h`,k}$ is the active power of house h` at time step k; $Q_{h`,k}$ is the reactive power of house h` at time step k; $a_{h,h`}$ is the influence of the active power of house h` on house h; $b_{h,h`}$ is the influence of the reactive power of house h` on house h.

$$V_{h,k} = V_k^0 + \sum_{h`=1}^{N} a_{h,h`} P_{h`,k} + \sum_{h`=1}^{N} b_{h,h`} Q_{h`,k} \quad (1)$$

The influences $a_{h,h`}$ and $b_{h,h`}$ have to be determined by solving a linear least squares problem. Considering the technical losses, the influences are calculated for the time steps without theft in order to identify the phase of each house. After identifying the network, the voltage at each house can be calculated by using equation (1). A large error between the measured and the estimated voltages for a given phase implies that a theft has been attempted on that phase. Normally, for the theft location, the difference is comparatively greater than other locations.

2.3 Simulations

Different cases were considered for the simulations as follows:

Case 1: Without Theft

The model was simulated without any theft in the network so as to compare the measured and expected voltage profiles. The percentage voltage errors were calculated for all the houses. The simulation was run for 1000 time steps representing the different time frames during which data was collected from the meters.

Case 2: Single Point of Theft on Feeder

An illegal load was connected at house 15, with the active illegal power varied from 150 W to 3750 W in steps of 150 W for every 40 time steps starting at time step 0.

Case 3: Single Point of Theft on each Phase

Theft was simulated as shown in Table-2.

Table-2: Single point of theft on each phase

House number	Phase	Illegal active power (kW)	Time steps of theft
15	C	2	1 to 1000
16	A	1	401 to 1000
17	B	3	601 to 620

Case 4: Two Points of Theft on One Phase

Theft was simulated as shown in Table-3

Table-3: Two points of theft on one phase

House number	Phase	Illegal active power (kW)	Time steps of theft
16	A	2	1 to 1000
34	A	3	401 to 900

Case 5: Presence of Distributed Generator (DG) in the Network

Several distributed generators were connected across the network as per Table-4.

Table-4: DG connections

House number	Phase	DG active power (kW)
10	A	1

| 11 | B | 2 |
| 12 | C | 5 |

The effect of the generators on the voltage profiles were initially analysed without theft. The algorithm was subsequently tested for thefts of 2 kW and 3 kW at houses 10 and 17 respectively during all the time steps.

3. RESULTS AND DISCUSSIONS

3.1 Case 1: Without Theft

The maximum technical losses in the network was determined from the power records of all meters and found to be 3 % on each phase. This value was used as a benchmark to detect illegal electricity consumption. Moreover, the influences were determined for all the phases to identify the houses on each of the three phases. Chart-1 shows the influence of active power of all houses on the voltage magnitude of house 15. All the houses connected on the same phase as house 15 can be identified and confirmed from Fig-1. A similar plot was obtained for the influence of reactive power.
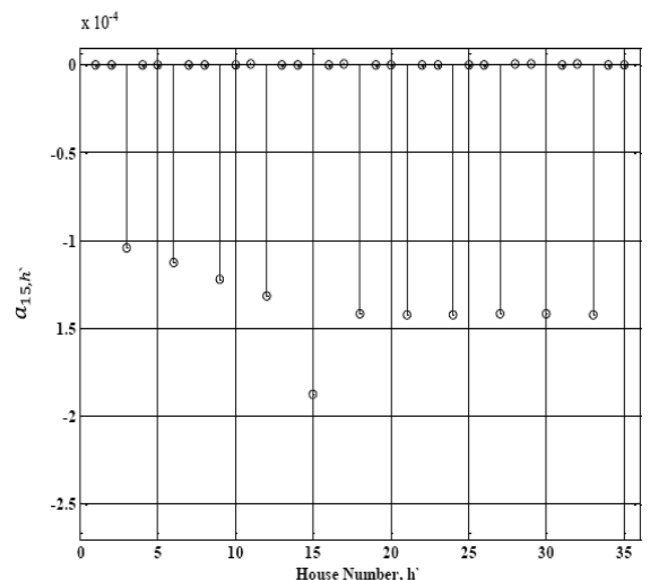

Chart -1: Influence of active power of all houses on house 15

The percentage voltage errors obtained for all the houses were very small (between 0 % and 0.008 %) and are displayed in Chart-2. Expected and measured voltage profiles for phase B at time step 500 are shown in Chart-3. It can be observed that the voltage errors were very small. Similar charts were obtained for the remaining two phases.
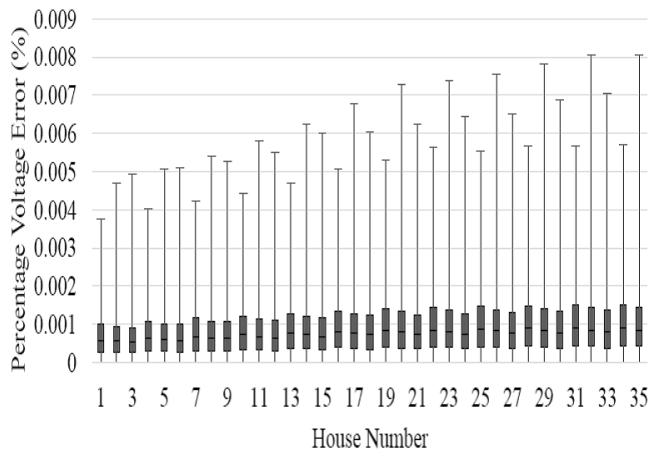
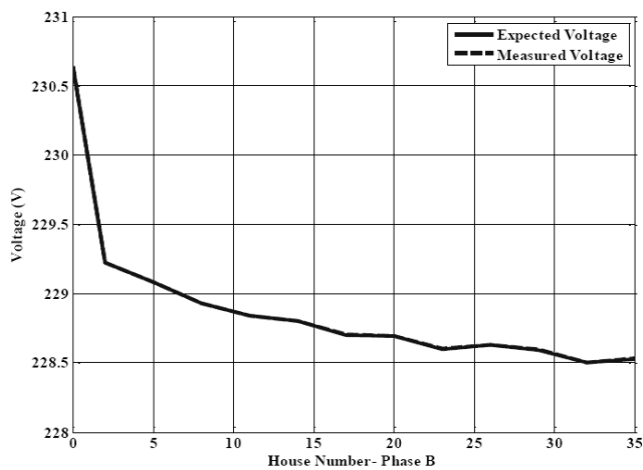**Chart-2**: Percentage voltage error for all houses at time step 500

Chart-3: Voltage profiles for phase B at time step 500

3.2 Case 2: Single Point of Theft on Feeder

Taking into account the 3 % technical losses, it was found that the minimum stolen power detectable was 450 W based on the increment of 150 W for every 40 time steps. The voltage and percentage voltage error profiles for time step 81 are shown in Chart-4 and Chart-5 respectively.
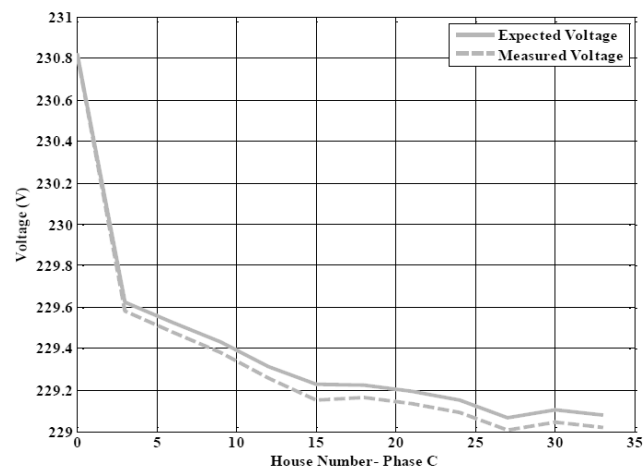

Chart-4: Voltage profiles for phase C at time step 81

Chart-4 shows that a theft occurred on the system as the measured and expected voltage profiles are no longer superimposed on each other. Chart-5 depicts that the theft occurred at house 15 as the corresponding percentage voltage error is maximum. The same conclusions could be drawn for profiles at time steps greater than 40, but with the percentage voltage errors being higher due to increasing stolen power at house 15.

3.3 Case 3: Single Point of Theft on Each Phase

The thefts at all the three houses were detected and located successfully at the corresponding time steps. The charts used for analysis were similar to Chart-4 and Chart-5.
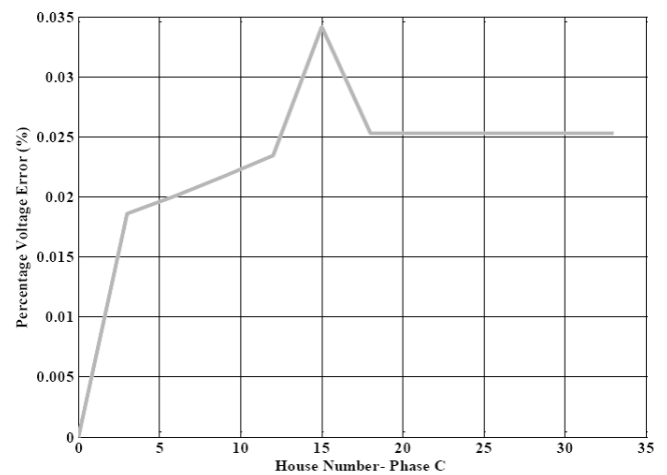

Chart-5: Percentage voltage error profile for phase C at time step 81

3.4 Case 4: Two Points of Theft on One Phase

The algorithm successfully detected and localised all points of illegal abstraction as shown in Chart-6 and Chart-7.
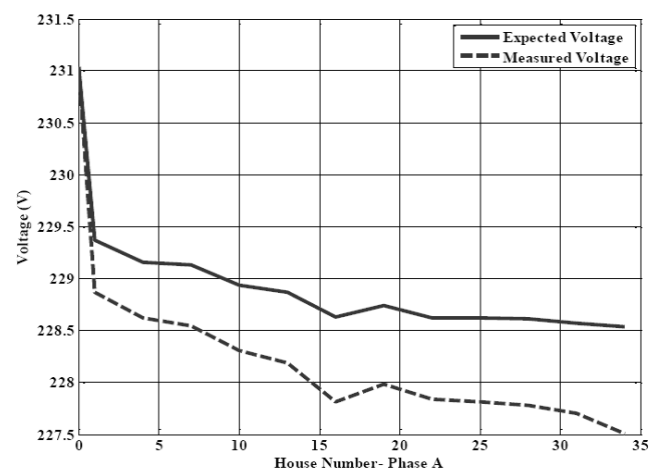

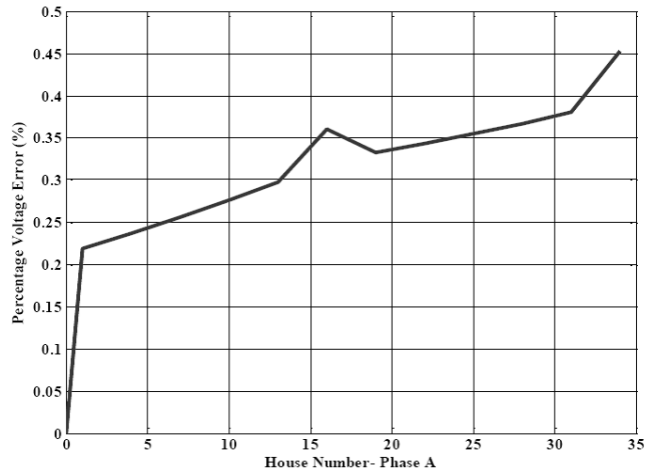**Chart-6**: Voltage profiles for phase A at time step 500

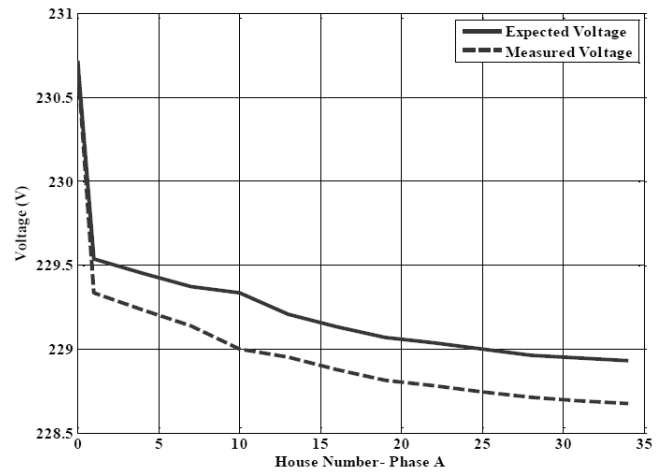**Chart-7**: Percentage voltage error profile for phase A at time step500

3.5 Case 5: Presence of DG in the Network

The voltage profiles in the absence of electricity theft for phase C at time step 500 are shown in Chart-8. The peak at house 12 is due to the relatively high power of 5 kW injected into the network by the DG of the house. The voltage errors can be observed to be very small.
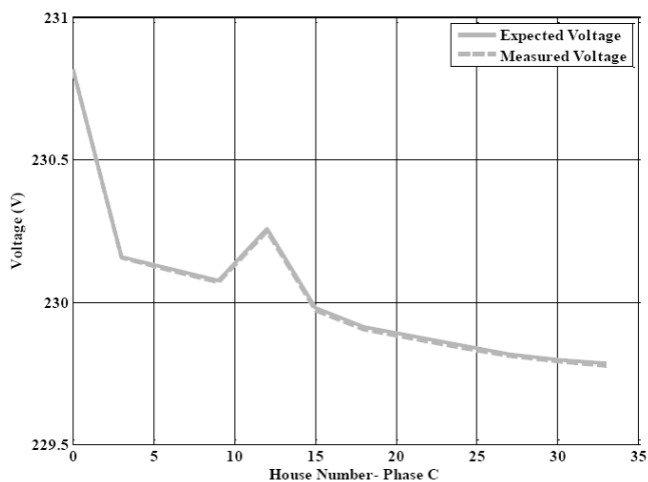

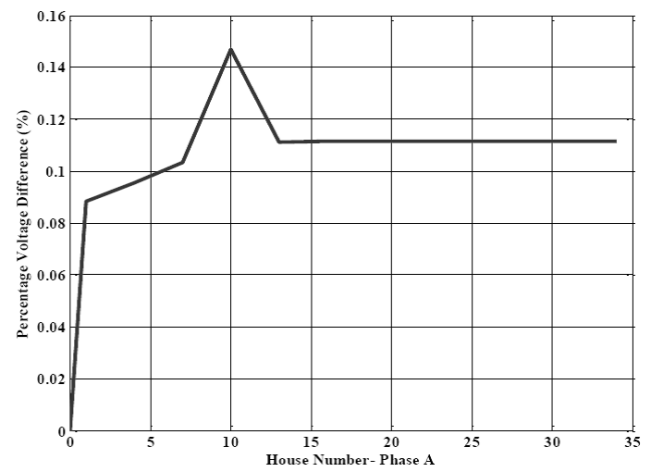**Chart-8**: Voltage profiles for phase C at time step 500

In the presence of electricity thefts, Chart-9 and Chart-11 clearly point out the presence of theft due to relatively large errors between the measured and estimated voltages. Chart-10 and Chart-12 show that the theft locations were successfully identified.
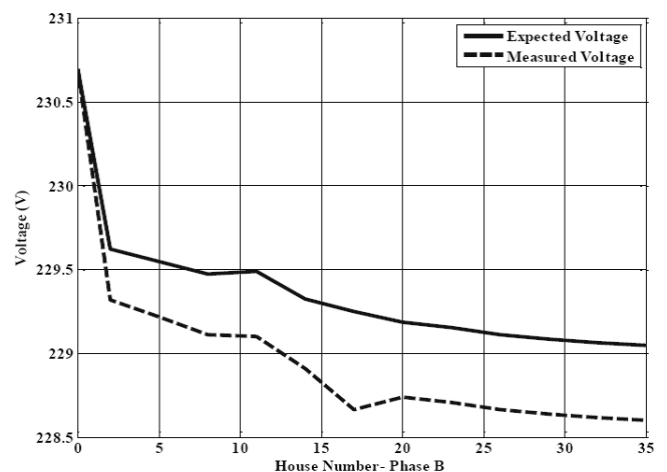

Chart-9: Voltage profiles for phase A at time step 500

Chart-10: Percentage voltage error profile for phase A at time step 500

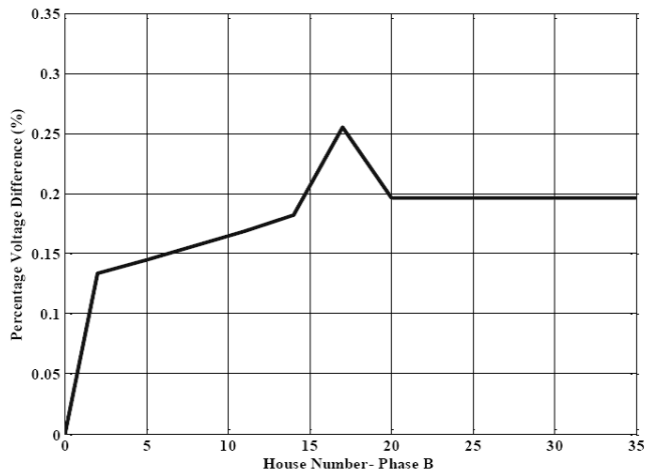**Chart-11**: Voltage profiles for phase B at time step 500

Chart-12: Percentage voltage error profile for phase B at time step 500

4. CONCLUSION

Smart meters incorporating the tested algorithm will be efficient in detecting single, multiple multi-phase and multiple single-phase electricity thefts in a radial low voltage network, both in the presence and in the absence of distributed generators, even if the network design parameters are unknown.

REFERENCES

[1] Frank Van Der Bergh, Petr Kadurek, Sjef Cobben, and Wil Kling, "ELECTRICITY THEFT LOCALIZATION BASED ON SMART METERING," in 21st International Conference on Electricity Distribution, Frankfurt, 2011, pp. 1-4.

[2] Thomas B Smith, "Electricity theft: a comparative analysis," Energy Policy, vol. 32, no. 18, pp. 2067-2076, August 2004.

[3] P. Kadurek, J. Blom, J. F.G. Cobben, and W. L. Kling, "Theft detection and smart metering practices and expectations in the Netherlands," in Proceedings of the Innovative Smart Grid Technologies Europe Conference, Gothenburg, 2010, pp. 1-6.

[4] R. Alves, P. Casanova, E. Quirogas, O. Ravelo, and W. Gimenez, "Reduction of non-technical losses by modernization and updating of measurement systems," in 2006 IEEE/PES Transmission & Distribution Conference & Exposition: Latin America, Caracas, 2006, pp. 1-5.

[5] University of Texas at Austin - Center for Electromechanics. (2011, September) Simulink Smartgrid Simulation 1: The Basics. Video (Youtube).

[6] Sam Weckx, Carlos Gonzalez, Jeroen Tant, Tom De Rybel, and Johan Driesen, "Parameter identification of unknown radial grids for theft detection," in Innovative Smart Grid Technologies (ISGT Europe), 2012 3rd IEEE PES International Conference and Exhibition on, Berlin, 2012, pp. 1-6.