ENERGY METER READING AND TAMPERING PROTECTION THROUGH POWERLINE COMMUNICATION CHANNEL

S. Naiman and M.M. Kissaka
Department of Telecommunications Engineering
Faculty of Electrical and Computer Systems Engineering
University of Dar es Salaam
P.O. Box 35131, Dar es Salaam, Tanzania.

N. H. Mvungi
Department of Computer and Systems Engineering
Faculty of Electrical and Computer Systems Engineering
University of Dar es Salaam
P.O. Box 35131, Dar es Salaam, Tanzania

Power utility companies have suffered revenue losses due to uncollected bills and energy tampering for many years. The use of powerline communication to overcome the problems has been proposed. This needs tampering detection and transceivers capable of communicating data through powerline channel. This paper identifies different methods of tampering, presents simulated results for tampering detection scheme and proposes a Direct Sequence Spread Spectrum (DSSS) with Binary Phase Shift Keying (BPSK) transceiver design for energy metering as a solution to the problem. The choice of DSSS-BPSK modulation scheme is based on its robustness and its ability to spread signal into wide band to protect jamming and interference. The performance of the designed tampering detection, transceiver and selection of suitable parameters is performed by using MATLAB software.

Keywords: *Metering technologies, power tampering, two -way communication*

INTRODUCTION

The power utility companies use different methods to determine energy consumed by its customers. These methods includes manual meter reading, estimation, prepaid meter, computerized hand held recording devices, remote electronic meter reading, drive by or mobile radio-meter reading and full remote monitoring or automatic meter reading (AMR). Most of these methods have inherent problems such as delays in billing, wrong estimates, meter tampering, huge cost of disconnection and re-connection for non-paying customers, difficult to access or in-accessible meters and power tampering. These are potential sources of revenue losses. The magnitude of revenue losses in some parts of the world are as follows; USA 4%, Pakistan in exceed of 35%, S. Africa over 38% of the sales, India over 10% of the sales and UK £250 million per year[1]. On the average the African power utility companies' losses are estimated to be 35% of sales per annum [2].

Tampering is the main source of revenue losses. Tampering techniques used in power utilities industry have been and continue to be identified. Tampering practices include those involving

direct tapping from powerline and tampering the metering unit. Direct tapping is the most common. It is done at high and low voltage powerlines causing huge revenue losses since it can go undetected for a long time. The metering unit tampering involves tampering with terminal seal, breaking control wires and partial/total meter shunting to reduce or eliminate meter reading. Other methods used, are breaking the voltage taps, switching CT wires and increasing aluminum disc eddy current. Access to internal part of meter to regulate readings is possible when meter seal is tampered with. The meter tampering in electromechanical meters includes obstructing mechanically the spinning disc, increasing breaking magnetic field using calibration screw, blocking the axis to stop registration and turning back the dials to reduce meter reading. The electronic meter readings can be reduced by removing voltage sensor, by interchanging phase and neutral current connection and scaling down voltage and current signals to the meter referred to as earth tampering. Other method of electricity theft/tampering includes tapping off a nearby paying consumer, damaging meter enclosures, turning the meter upside-down (i.e. interchanging of the incoming and outgoing or live and neutral).

Different solutions have been thought to overcome these problems. In an effort to solve these problems in developed countries, various metering systems have been adopted such as computerized hand held recording devices, remote electronic meter reading, drive by or mobile radio-meter reading, prepayment-metering systems and a full remote monitoring or automatic meter reading. Automatic meter reading is perceived as an appropriate means to overcome energy theft and to raise revenue collection by power utility companies. The use of full remote monitoring systems through powerline Network with an intelligent transceiver meter is proposed as cost effective solution to address the above problems in developing countries. This is due to availability of powerline network for all electricity users and the network belongs to power utility. The system in consideration is from customer meter to distribution transformer and bypassing a distribution transformer to primary substations. The need for bypassing a distribution transformer is due to lack of communications link in most of distribution transformers. The general network layout is explained in [6]. However, network topology presents challenges in general communication system design. These include energy meter with transceiver design and appropriate media access control and identification.

In this paper the design of an intelligent meter that incorporates tampering detection circuit and a two-way communication facility is discussed. Tampering detection is based on monitoring of live and neutral currents, and voltage. Design of transceiver has been considered as necessary for remote monitoring of tampering status. The transceiver parameters have been tailored to enable communication at low cost considering the nature of powerline channel. Moreover, appropriate modulation scheme has to be determined to maximize throughput.

PROPOSED SOLUTION

To eliminate problem of revenue losses and that of tampering in Power utility companies, the use of intelligent meter with a two-way communication and tampering detection facilities is considered necessary. Hence, the design of tampering detection circuit and transceiver through powerline is required.

Design of Tampering Detection

The analysis on the factors and means that are necessary to eliminate tampering has led to the conclusion that to detect tampering, one need to monitor three parameters, these are live and neutral currents and input voltage to the energy meter. It is therefore advocated to migrate from electromechanical meters to electronics ones with transceiver as shown in figure 1.The tampering detection concept is simulated as shown in figure 2 to evaluate response of designed tampering detection scheme. The output indicates the kind of tampering affected.

The possible outputs of the fraud/theft sensing (logic) circuit simulated that shall be sent to the

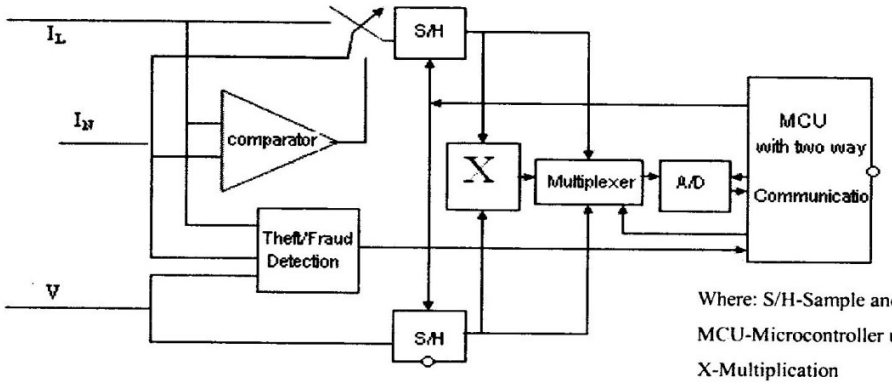


Figure 1: Block diagram of the proposed solution to the tampering and communication in energy metering

MCU for transmission to the control center are *missing potential (PT), earth tampering (ET), current reverse (CR) and Outage.* Comparison

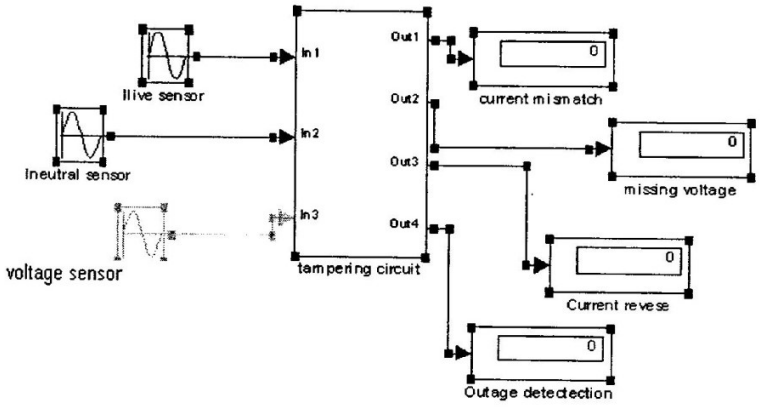


Figure 2: Circuit to simulate the possibility of controlling all kinds of tampering

between the inputs from the two current sensors and phase angle between current in live conductor and voltage is determined. The magnitude of input voltage is compared to some reference. Logic operations are then performed using all these factors to determine possible tampering action, the results of which are as given in table 1 in appendix 1.

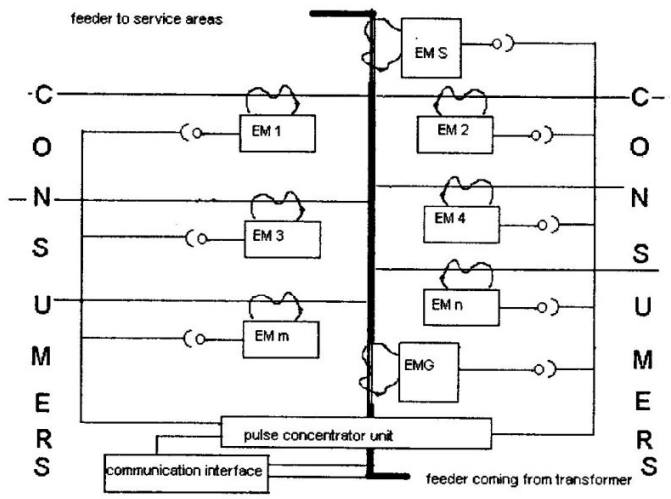
The proposed network to facilitate the detection of all kinds of tampering in the metering system is as shown in figure 3. With this network configuration, energy theft through action in the metering system and that of tapping from power line can be arrested. It is also a good solution for efficient and effective revenue collection. Tampering action can trigger transmission of alert signal to the power utility billing and technical centers through the powerline channel. The tampering problems such as directly connection to power supply bypassing the meter can be overcome by checking meter EGM that feeds a number of customers show in figure 3. The simulation result suggests that it is possible with this scheme to detect all kinds of tampering attempts.

Design of Communication Transceiver

The schematic diagram of the energy meter transceiver designed for powerline communication is shown in figure 4 where DSSS-BPSK modulation is used. The switch is incorporated for the purpose of automatic connection and disconnection remotely and for responding to tampering actions. The isolation of transceiver from high voltage is achieved via the coupling circuit.

BPSK Modem System

The BPSK modulation scheme has been identified as being suitable for data transmission through powerline. The BPSK modulation was chosen for the powerline modem because it is



Where: EM –Customer Meter, EMS- Energy meter for service Area, EGM- Energy meter for global consumption

Figure 3: Layout of proposed Remote Monitoring System, which can eliminate tampering and billing problems

insensitive to narrowband disturbances, has selective attenuation, works well with low signal power and has forward error coding through spreading and dispreading therefore providing robustness to noise in the channel [5]. The transceiver for energy metering using BPSK modulation is shown in figure 5 and 6. The transmitter transmits information at 10kbps through coding block where PN code generator of 15 chips is applied and then the BPSK modulator is applied before the signal is introduced to the channel. The receiver has synchronization block, BPSK demodulator, decoder and PN code generator, which is identical to that of the transmitter. The transceiver has been simulated using matlab.

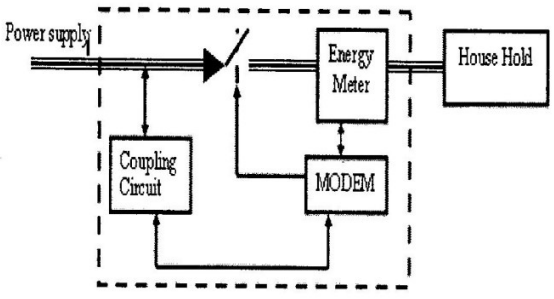


Figure 4: Layout of energy meter reading through PLC

Transceiver Parameter

For effective transmission of data, the network was designed with receiver/repeater positioned at every 400 meters [6]. The aim is to transmit and receive data at 400 meter with BER of 10^{-8}. Hence, the transceiver parameters like PN code generator, chip rate, receiver sensitivity, bandwidth, data rate, processing gain and receiver SNR had to be selected appropriately. The maximum length sequence (M sequence) from PN generator was chosen due to its good autocorrelation characteristics and easiness of implementation. The spreading code period is given by equation (1) where N represents a spreading factor and k is number of bits. The value of k was found to be 15 (15-chip PN sequence), which gives spreading factor (N) of 32767.

$$N = 2^k - 1 \quad (1)$$

The data rate (r_b) of 10kbps was determined to be enough for meter reading and tampering control purpose [6]. Hence, the required bandwidth (B_T) for the signal to be transmitted through powerline is 5 kHz. This is calculated using equation (2), where w is a factor, which relates bandwidth and channel properties with different modulation scheme. For the BPSK modulation scheme it was taken to be 0.5.

$$B_T = w r_b \quad (2)$$

Using equation (3) the system chip rate (r_c) of 327.67Mcps was chosen.

$$r_c = N r_b \quad (3)$$

Processing Gain

The processing gain (PG) calculated using equation (4) is 45dB [7]. The simulated results in figure 7 and that in table 2 confirm the suitability of 45dB as PG and that the higher the PG the better is the BER.

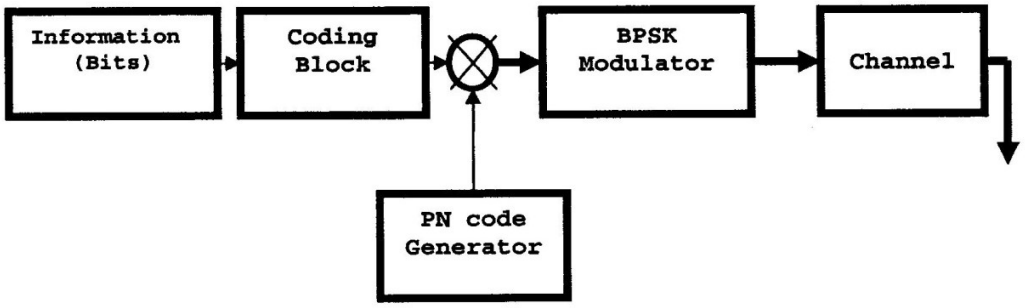


Figure 5: Transmitter Block diagram

$$PG = 10 \log(\frac{r_c}{r_b}) \quad (4)$$

Equation (5) gives the signal to noise ratio (SNR) of 15dB with $\frac{E_b}{N_o}$ as ratio of received signal power to noise power of 12dB. These values were obtained at the required BER.

$$SNR = (\frac{E_b}{N_o})(\frac{r_b}{B_T}) \quad (5)$$

Receiver Sensitivity

To optimize SNR, the receiver optimization for sensitivity and transmitter power parameters is required [8]. The receiver sensitivity P_r of $-110dB$ was obtained as calculated using equation (6) with noise floor (N_o) of $-125dB$ at the receiver.

$$P_r = N_o + SNR \quad (6)$$

The Noise floor (N_o) was calculated using equation (7) with N_F the noise figure assumed 15dB, B_T the channel bandwidth [Hz], T_A the ambient temperature, k_B the Boltzman's constant is 1.38×10^{-23} and N_B the background noise estimated at –140dB.

$$N_o = N_B + k_B T_A B_T + N_F \quad (7)$$

The receiver sensitivity shows the required minimum received signal power at receiver for demodulation.

Transmitter Power

The minimum transmitted signal power was determined to be (P_{tx}) –20dB (10mW). The value was arrived at considering path loss /channel attenuation (PL), receiver sensitivity and fade margin (FM) as shown in equation (8).

$$P_{tx} = P_r + PL + FM \quad (8)$$

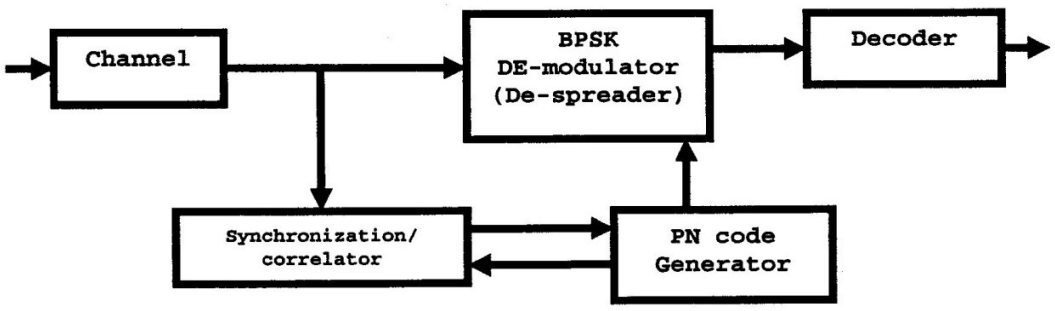


Figure 6: Receiver Block diagram

Path loss PL was estimated to be 60dB using equation (9), with **Error! Objects cannot be created from editing field codes.** as transfer function for powerline channel where **Error! Objects cannot be created from editing field codes.** are the transmitter/receiver distance, modulation frequency and number of interconnection in the channel respectively. The fade margin used is 30dB.

$$PL = 20 * \log_{10} |H(f,d,N)|^2 \, dB \quad (9)$$

For data communication through powerline, the maximum permitted signal power is 500mW (CENELEC standard). This using equation (10), gives the optimal SNR of 32dB.

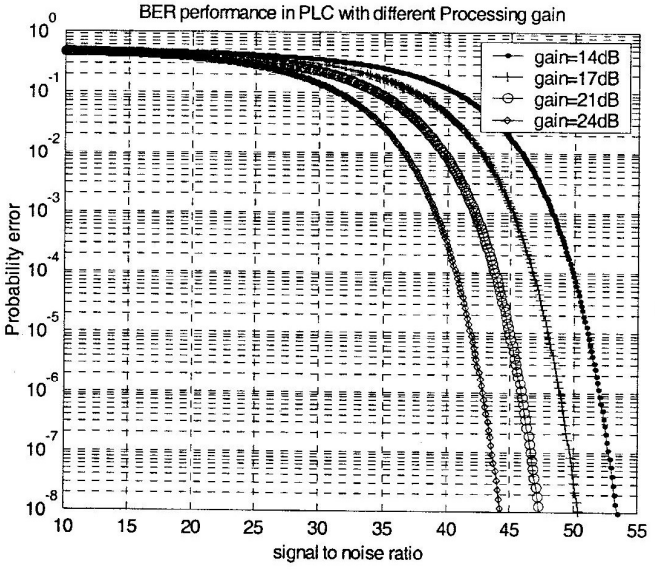


Figure 7: Simulated systems BER performance with different Processing gains

$$SNR = P_{tx} - PL - FM - N_o \quad (10)$$

SIMULATION RESULTS

Simulation of SNR versus BER for different PG given in figure 7 shows that with PG of 14dB, 17dB, 21dB and 24dB requires at least SNR of 54dB, 51dB, 47dB and 44dB respectively to effect the same BER. Result from table 2 shown in the appendix for different value of PG agree with that in figure 7 that the higher the

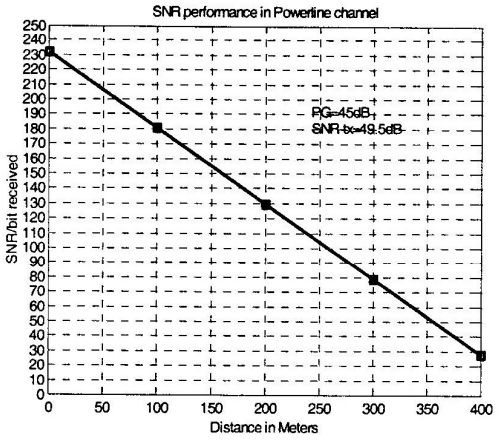


Figure 8: Variation of received SNR with distance in Powerline Channel

PG values the lower is the required SNR to achieve the same BER. To transmit signal to a distance of 400 meter with the required BER PG of 45dB is required. The variation of PG and transmitted signal power (SNR) with respect to improvement in BER at the distance of 400 meters were observed as shown in table 2 and figure 8,9 &10. The results shows that the required BER is achieved by increasing either the transmitted signal power (**Error! Objects cannot be created from editing field codes.**), PG

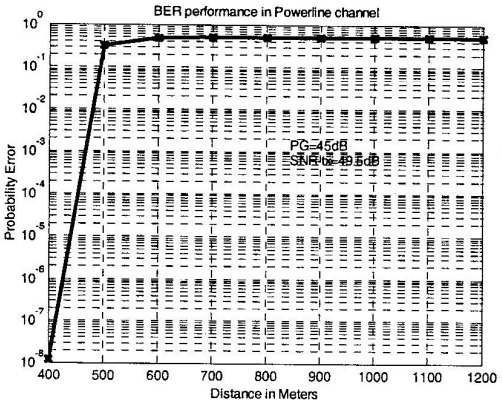


Figure 9: Variation of received SNR with distance in Powerline Channel

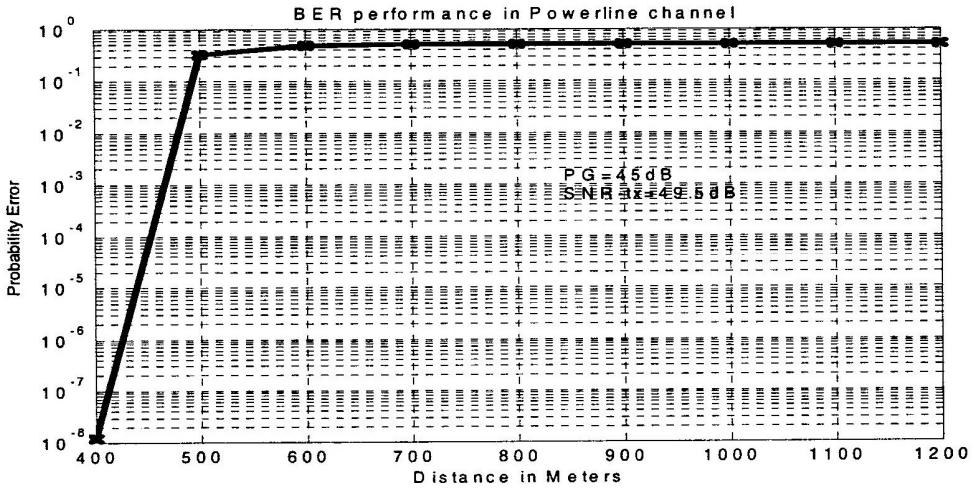


Figure 10: Variation of received SNR with distance in Powerline Channel

Table 1. Results from simulated circuit for detecting tampering

INPUTS			OUTPUTS			COMMENT	
I_{live}	$I_{neutral}$	Voltage	Potential Temaping	Earth Tampering	Current Reverse	outage	
5	3.1	230	0	1	0	0	E T
-5	3.2	230	0	0	1	0	CT
-5	6.8	220	0	0	1	0	CT
5	6.9	225	0	1	0	0	E T
10	8.1	215	0	1	0	0	E T
10	10	206	1	0	0	0	PT
-10	11.8	213	0	0	1	0	CR
50	48.1	237	1	1	0	0	ET
-50	48.2	230	0	0	1	0	CR
50	50	230	0	0	0	0	NT
-50	51.8	230	0	0	1	0	CR
50	51.9	230	0	1	0	0	ET
85	86.8	235	0	0	0	0	NT
4	5	199	1	0	0	0	PT
5	5	180	1	0	0	0	PT
1.7	2	190	1	0	0	1	outage
1.8	1.9	201	1	0	0	1	outage

or both of them. However, care must be taken in the case

of increasing transmitted power, since its increase is associated with increase in transmitter complexity. With the target of achieving demodulation at 400 meter with BER of 10-8 and maximum SNR of 32dB, the simulation shows that PG of 45dB (15-chip sequence) and SNR of 28dB is required.

CONCLUSION

In this paper the design of energy meter with transceiver has been presented. From the simulation results for tampering detection circuit

and transceiver circuit, it is concluded that by monitoring three parameters that are essential for energy measurements (live current, neutral current and voltage) tampering actions/attempts can be detected. These actions and the energy metered data has to be transmitted to utilities control center through the noisily powerline channel to realize a PLC based ARM system.

When a receiver is placed at 400 meter in the low voltage (secondary) distribution network, the data transmission is achieved at a rate of 10kbps with BER of 10-8 using BPSK modulation scheme. The chip rate of 327.67Mcps with processing gain of 45dB and SNR at receiver of 28dB with receiver sensitivity of –110dB and minimum transmitting power of –20dB was realized.

Table 2: variation of BER with the change in PG and transmitted signal power at a distance of 400 meter

$SNR_{tx}(dB)$	SNR_{rx} **in dB**	*PG* **in dB**	*BER*
60	5	20	10^{-8}
60	5	20.7	10^{-10}
55	-5	20.7	10^{-4}
55	-5	21	10^{-4}
55	-3.5	21.7	10^{-5}
55	0	23	10^{-6}
55	3	24.7	10^{-8}
55	6	26	10^{-11}
45	-17	26	10^{-2}
45	-14	27	10^{-2}
45	-7	30	10^{-3}
45	0	33	10^{-6}
45	4	34.7	10^{-8}
45	6.5	36	10^{-10}
35	-16.5	36	10^{-1}
35	-15	36.9	10^{-2}
35	-10	39	10^{-3}
35	-5	40.8	10^{-4}
35	-3	42	10^{-5}
35	0	43	10^{-6}
35	0	43.4	10^{-6}
35	2	44.1	10^{-7}
35	4	44.8	10^{-8}

REFERENCES

1. S. Singhal, ''The Role of Metering in Revenue Protection'', PRI Ltd, U.K, 1995.
2. D.Louw, ''African Revenue Protection Association Update'', ESI Africa, The Power Journal of Africa, Issue 4, 2001, pp 21.
3. J .S. Michael, "AMR - the cure for energy theft'', Metering International, Issue 3, 1999.
4. Sloan ''Current Affairs - Prepayment a Viable Solution to Energy Theft'' Metering International, issue 4, 1998
5. J.G. Proakis ''Digital Communications'' McGraw-Hill Series in Electrical and Computer Engineering, Third Edition, pp 695-753, 1995.
6. J. Anatory, ''Investigation of Appropriate Technology for Remote Monitoring of Electrical Power Consumption in Tanzania", Thesis submitted in fulfillment of Master of Science in Engineering (Electrical), University of Dar es Salaam, Tanzania, November 2003.
7. J.Meel,''Spread Spectrum''Sirius Communications Hogeschool Voor Wetenschap & Kunst, Dec 1999
8. J.Zyren and A. Petrick, ''Tutorial on Basic Link Budget Analysis'' *Intersil*, Application note, June 1998