Curbing Electricity Theft Using Wireless Technique with Communication Constraints

Salome C. Tshikomba, Milton Estrice, Evans Ojo and Innocent E Davidson
Department of Electrical Power Engineering
Durban University of Technology
Durban, 4000, South Africa
innocentd@dut.ac.za

***Abstract*— Utility services are experiencing a common problem of power losses, which impose a significant impact on their annual budget. Practically, power losses consist of technical losses and non-technical losses. Technical losses are due to operations and aging of infrastructure, while non-technical losses (NTL) are due to non-metered energy. The focus is on managing non-technical losses using an automation wireless method. The wireless ZigBee technique is proposed and further investigated for communication failure over long distances while solving the problem of stealing electricity. Advance-metering infrastructure (AMI) technique and smart meters are feasible for system integration; that is why they are chosen to be part of this study. The success of the study depends on quality data of the Utility, meaning the more accurate the data, the easier the analysis of outliers. The operation and planning of revenue protection contain a large amount of data that needs to be worked on, so data mining assists in that regard. Then the load profiling method assists in illustrating the variation in demand/electrical load over a specific time. This is a preliminary investigation using a wireless communication technique as a viable solution in curbing electricity theft. The uniqueness of the proposed ZigBee system is that it recognizes the everyday act of stealing electricity through tempering with the meter box and tapping of the supply.**

Keywords*— Losses, smart meters, AMI, wireless technique, ZigBee technology, NTL.

I. Introduction

The provision of electricity is a basic need or an exercise of human rights in South Africa. The leading utility suppliers in South Africa are Eskom and municipalities. Eskom and municipalities should ensure that most of the citizens are supplied with electricity. This also includes rural areas, irrespective of the financial standing of anyone, or the prevalence of poverty in households. This is because the affordability of electricity in South Africa is a sine qua non. Eskom is the largest generator of energy in South Africa. Still, it is the least distributor of energy to the end-users; in some areas, it shares the service delivery with municipalities, which as well creates complex situations when service delivery problems arise. Theft of electricity poses a grave danger to Eskom and the municipalities with overwhelming impact; South Africa's economic growth is challenging to maintain, placing pressure on the country's annual revenues, which could be used for other important development projects. Every year, electrocution due to theft of electricity via unsafe, illegal connections and meter tempering causes many public fatalities. Innocent young children are the victims most.

The consequence of electricity theft is higher tariffs for all. Other effects include power outages, production downtime, traffic street lights failure, household inconvenience, damage to appliances, etc. The objective of the study is to analyses non-technical losses (NTL) and utilized the ZigBee technique as the solution for curbing illegal electricity connections, being conscious of communication problems over a long distance. The structure of the paper is as follows; Load profiling and data mining, advanced metering infrastructure (AMI), smart metering, and ZigBee technique with its network communication.

II. Research Methodology

The procedure is to collect data correctly, preserved data and processed it properly, for analysis and interpretation

- A pilot study using existing infrastructure with the ZigBee technique implemented to curb electricity theft.
- The load profiling, AMI, smart meter play essential roles in the interfacing of the ZigBee technique to the existing infrastructure.
- To evaluate the feasibility of the project, a survey using a questionnaire administered to respondents, and the losses and cost associated estimated.
- An investigation into incidents of communication failure.

III. Energy Loss Analysis

Utilities describe energy loss as the difference between the energy obtained as measured in the transmission networks and the energy sold to all clients. Those losses are experienced in technical and non-technical terms:

A. Technical Losses

A technical loss is a loss inherent in the system and refers to the energy lost in the electrical networks because of the current flow or the system's energization [1] [2] [3].

Electricity and energy are lost from the distribution system. As electricity flows through substation conductors, heating occurs, which energizes the transformer. When transformers are energized, hysteresis/losses occur in the transformer core, all of which contribute to the loss of electrical energy [2][4]. Long distribution lines also contribute to the technical losses: overloaded distribution lines contribute to losses as the lines or cables lose energy through heat generated [5]. Aging distribution infrastructure due to short circuits can also bring about losses.

B. Technical Losses

These are caused by electricity theft resulting from illegal tapping from Utility's infrastructure, network, or bridging of the meters and incorrect billing or non-billing of the customers [5] [6] [7]. Some factors may lead to non-technical

978-1-7281-6770-1/20/$31.00 ©2020 IEEE

losses. On the customer data that is received from the municipality, there are business customers that are sitting on a residential segmentation tariff. Those businesses are under-billed by paying residential tariffs instead of business tariffs because business tariff includes fixed charges, which are paid monthly without fail. The incorrect K-factor is another cause of revenue loss that can cause the municipality to lose revenue. In some municipalities, the billing data that was analyzed, several industrial customers were registered with wrong K-factors, for example, on 0.02, 0.04, 0.06, 0.08, and 0.12, in the billing system. The K-factors are based on the voltage ratio and current transformer ratio of the customer [6] [8].

IV. NTL Load Profiling and Data Mining

The customer's load consumption pattern over a given period (load profiling) assists the Utility to understand the characteristics of their customer's load consumption, this helps to reveal an irregular pattern of use strongly associated with NTL activities [4][6].

A. Benefits of load profiling method

- It yields good results and is the most cheaper approach compared to other existing techniques that can trend energy consumed.
- Assist Utility Companies in determining the next financial budget plan.
- It assists the power Utilities in reviewing marketing strategies to improve efficiency.

B. Loading conditions

The need to evaluate and analyze loading conditions is crucial in ascertaining losses because different load situations create various load types from one customer to the next. As shown in Table 1 the loading conditions are.

TABLE I. Loading Conditions [4]

Loading conditions	Items
Type of customer	Domestic
	Commercial
	Industrial
Location	Urban
	Rural
Voltage level	Low Voltage
	Medium Voltage
	High Voltage
Type of climate	Rainy or windy
	Hot or Cold
Type of day	Week day
	Weekend (Saturday and Sunday)
	Public holiday

C. Selection of Data

While selecting customers, it's quite necessary to observe these criteria:

- Duration of the invoices measured, e.g., monthly.
- Topographical position, for example, is urban or suburban.
- Contractual tariff structure: Single phase domestic, three-phase domestic, large power users, and high tension users.
- Economic activity classification; if the area is well off in terms of business or there is a high rate of unemployment, which can cause a high rate of NTLs [9].

V. Fuzzy Logic Control Design

Advanced metering infrastructure includes a smart grid and consists of a mixture of functional and energy controls, intelligent devices, smart meters, clean energy resources. The smart grid is preferred because it is easily integrated with other new techniques of curbing the stealing of electricity. A smart grid can also achieve the following [10] [11]:

- Distributed resource integration (DER) and generation deployment of DER along with renewable resources.
- The use of digital knowledge is improving. This control innovation can enhance protection, stability, and the performance of the electric grid.
- The complicated optimization of the grid activities will take place under maximum cybersecurity
- Incorporated and built efficient energy tools, demand-side tools, and market response.
- Consumer equipment and smart appliances combined.
- Offering monitoring choices and timely information to customers.
- Using smart technologies, it can mechanically automate consumer products and other appliances. It tracks the contact issues, their activities, and distribution automation.
- The integration of modern electrical storage and cutting edge technology with the conventional plug-in and hybrid electric vehicles used.
- Change in the quality of connectivity, the operation of the devices, and the electrical grid linked systems and the grid infrastructure.
- Integrating AMI and drastically reducing needless obstacles will lead to smart grid technology, services, and practices being embraced. AMI represents the first step in the smart grid [10].

A. Importance of AMI

Advanced metering infrastructure (AMI) is utilized by power Utilities because it can be redesigned and still perform the way it should be. The smart meter system is an integral part of AMI which cater for data collection and communication. The smart grid is feasible for monitoring of the delivered energy. It is a unique system that allows customers to monitor their own consumption via the computer program [10]. If used concurrently on the network, AMI with Programmable Logic Controllers (PLC) can be viable for two-way communication between the meter and remote terminal unit (RTU) of the central station, located at the nearby substation. In the case of meters (sensors) tempering, it sends a warning signal to the central station, shut off meters for a long time. It has a meter kill-button at the central station, power line contact capabilities, and data logging capabilities (signature analysis, receiving, sending) and lower cost [5] [10].

VI. Smart Meter and ZIGBEE Technology

During outages, the smart meters detect and restore energy faster to the customers. Smart meters are capable of reducing the demand in energy supply, which will automatically stop unnecessary projects of building new substations. The smart meter can also reduce greenhouse gas emissions and other pollutions [10] [11].

The ZigBee technology is used because it is capable of limiting the problems associated with confined space in rural areas where it is challenging to install the wired information system. A mobile phone is used to send messages to officials. Many wireless technologies, such as infrared and Bluetooth, have range and performance limitations. Utilities pay a license fee to get access to GSM / GPRS, and the hardware costs are very high. It uses an unapproved 2,4 GHz ISM band available around the world. ZigBee extends from 10 m to 2 km, which operates well with networks like Wi-Fi, Ethernet with GPS. It also offers a flexible networking platform, which makes it ideal for application control and monitoring [12].

ZigBee consists of the following three devices [12].

A. The ZigBee Application

- It is a ZIGBEE device that starts the signal. It schedules the signal at the transmitting point and quickly transmits the signal.
- The ZigBee infrastructure only has one coach.
- The system has a particular networking tree and links to other systems.
- It can archive network information, including it, acts as a security key database.

B. ZigBee Device Router

- It offers the signal path at the time it is transmitted.
- ZigBee is a type of linear device which can route signals from one point to the next.
- Routers can function as a transitional router that transmits data from other systems.

C. ZigBee terminal device

- There is no routing functionality at this portion. Just sending and receiving data to act on.
- The end system acts as a leaf node in a network cluster tree.
- All terminal devices except the coordinator are access points in a star network.
- The battery has a long service life.
- A full mesh network does not include end devices, but, in reality, one or more of them might be needed by design.
- In the end, it's there.
- It has sufficient flexibility to communicate to its parent node (whether it's a coordinator or a router); it cannot relay data between devices.
- It takes the least amount of storage and is less costly to produce than a ZC or ZR.

Figure 1 illustrates the ZigBee procedure flux. The flow chart illustrates how the device works to prevent the theft of electricity. Then, a microcontroller tests for the resistance, and if the resistance increases, the source is shut off and LCD indicates the meter is tempered. There is a need for an amplifier circuit to run the microcontroller via the relay, because there is no direct connection to the microcontroller by the relay. Once the microcontroller turns off the load, the ZigBee modem transfers the results to the official who has been approved. The device won't allow the user to reset. Could only be reset by approved personnel. The microcontroller transmits the information to the relay and turns OFF, while the device turns off the power supply to the meter. Then the LCD shows the "Meter balanced" message and that message reaches the official of the Utility. The cycle is outlined in Figure 1 [13].

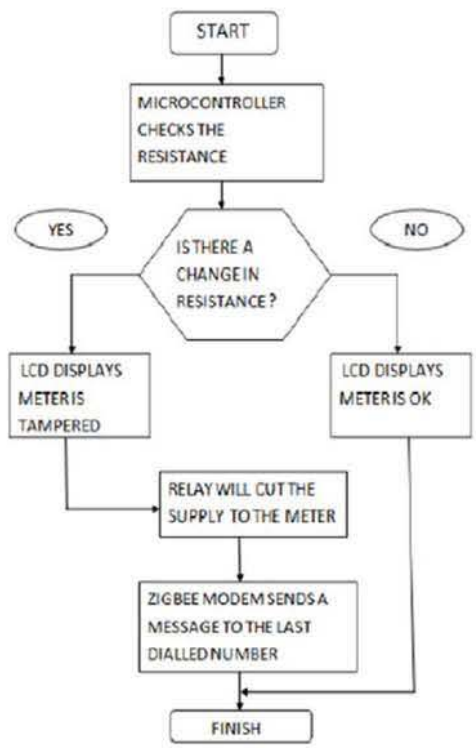

Fig. 1. ZigBee Process Flow

VII. Communication Network For Electricity Automation

The goal of electrical system automation is to maintain continuous power service to end-users. Power utilities find it challenging to supply reliable power without fail in both rural and urban areas because of unforeseen and natural catastrophes. Electric utilities need faster and secure network communication for their operational and commercial requirements to integrate or synchronize with existing equipment and planned functional equipment. The communication technologies consist of four classes as follows; power line, satellite, wireless, and optical fiber communication [14].

This offers significant benefits for electrical utilities, like low operating costs, minimal setup of the network, responsiveness, and consistent service coverage. For instance, small-power and minimal-range remote sensors may be used in city areas, WiMAX devices enabling a fully integrated computer network for electrical system automation and applications, including real-time grid and equipment monitoring and automated remote meter reading systems. Standard personal computers impose significant restrictions, as sensor nodes provide limited capacity for processing, storage, and energy. Wireless connections also have low bandwidth, and safety is essential and sometimes even essential for several sensor network technologies [14]. Another challenge is the budget because they are expensive to operate in urban areas. The changing technology can be a challenge since a customer cannot buy network connections but lease it or obtain a license to act on it for a specified period. Communication networks in rural and urban areas are crucial to electricity automation.

VIII. SECURITY IN WIRELESS SENSOR NETWORK

This pilot study was conducted to clarify the protection of tiny sensor nodes and their privacy. The attainment of the goal remains a difficult task because of the limited capacity of the sensor nodes in terms of computation, storage memory, connectivity, and energy source [15]. The following are attacks on the sensor networks and potential defensive mechanisms and the following remedies [15]:

- Jamming (physical layer): lower duty cycle, spread-spectrum
- Manipulation (physical layer): vandal-proofing, active control of primary systems.
- Collision (links layer): code correcting errors
- Exhaustion (link layer): rate limit
- Corrupting information concerning routing (network layer): authorization, encryption
- Selective forwarding attack (network layer): latency, probing
- Sybil vulnerability (network layer): authentication
- Sinkhole attack (black hole) (web layer): authentication, tracking, scalability
- Wormhole intrusion (network layer): Robust route selection surveillance
- Hello (network layer) flood attack: two-way encryption, a three-way interaction
- Flooding (transport layer): restricting link numbers, puzzles for clients
- Clone attack (Application layer): single wise pair keys.

The limitation of the secure server system is when the server gets hacked, the network is absolutely unsafe. Though, the base station on which the server operates is presumed to be safe. It is very crucial to monitor and do target tracking [15].

IX. PILOT PROJECT STUDY RESULTS

TABLE II. BENEFITS OF THE CASE STUDY [4]

Customer	Aspiration	Utility
Control over consumption;	Control over illegal consumption;	Low/No revenue loss securing the financial sustainability of Utility
Fewer outages	Financial sustainability	High payment levels
Fewer safety incidents	Satisfied customers	Low /no outages due to overloading
Improved quality of supply	Customer controls energy consumption	Low maintenance costs;
Reliability of supply	Meter philosophy for all residential customers.(prepaid and/or smart meters)	High customer satisfaction index;
No estimations	Control over illegal consumption	High customer satisfaction index
No billing issues	Fairness to customers	Improved Operational Efficiencies.
Efficient use of electricity		

Note: The following costs are based on the pilot project (3000 units)

ZigBee Cost	
	Total Cost
Material Cost	R4,055,800.00
Design and Transport costs	R826,104.03
Overheads, Contigency and IDC	R1,776,905.57
Labour Costs	R1,823,400.00
Maintainance cost	R0.00
Grand Total	**R8,482,209.60**

Fig. 2. Cost of the ZigBee System

X. SURVEY RESULTS

A. Graphical Representation of Results

Results from the table to the graph are arranged as questions against the number of people. The light color blue represents strongly agree, red represents agree, purple represents not sure, yellow represents disagree while royal blue represents strongly agree.

TABLE III. OUTCOME OF SURVEY PER QUESTION

Ratings	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Strongly Agree	19	24	22	12	23	20	19	14	7	5
Agree	13	23	20	19	16	21	17	21	27	29
Not sure	8	1	5	10	6	3	4	10	13	7
Disagree	3	0	1	2	4	4	6	2	1	5
Strongly Disagree	7	2	2	7	1	2	4	3	2	4

TABLE IV. THE OUTCOME OF THE SURVEY PER QUESTION IN %

Ratings	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Strongly Agree	38	48	44	24	46	40	38	28	14	10
Agree	26	46	40	38	32	42	34	42	54	58
Not sure	16	2	10	20	12	6	8	20	26	14
Disagree	6	0	2	4	8	8	12	4	2	10
Strongly Disagree	14	4	4	14	2	4	8	6	4	8

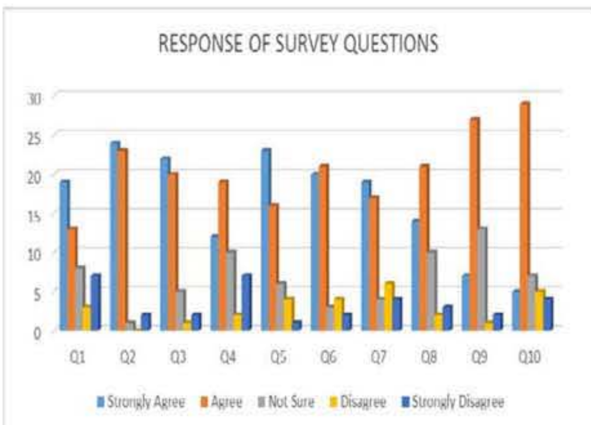

Fig. 3. Results of Survey

B. Discussion of Survey Results

It can be concluded that the survey questionnaire served the purpose because a large number of respondents did support the thesis idea. However, it was clear that most of the end-users lack knowledge about electricity infrastructures and the networks. A typical South African indigent citizen, also called the poor of the poorest (POP) do not understand the importance of cash flow, that is, the amount of money going into any organization and the amount which is coming out. The decision to do this survey manually was taken with such reason in mind so that if the customer does not understand, then the interviewer can assist a little bit in explaining some of the concept and attendant issues that the end-users are not sure or aware of. The critical situation that was noted is that, before interacting with the community. The first point of contact which cannot be omitted is to have access to local councilor whom they feel holds the responsibility to manage the affairs of the area because he/she was voted to bring service delivery to the people at all times.

The survey conducted is in tandem with the objective of the thesis. The research questions that were developed and tested provided a proven percentage score of positive responses to the questionnaire. Though some respondents were not straightforward because they are still happy with the current situation of things wherein they still hope to indulge in theft of utilities. They, therefore, saw the thesis as an avenue to rob them of freedom to continue the pilferage of electricity without any legal penalties imposed on them. The cost associated with energy losses that are caused by illegal electricity connections will decrease by upgrading the infrastructure, installing the ZigBee technique, and by giving attention to the communication system and its problems. The wellness and workshops need to be conducted so that communities at least once a month will learn the basics of the danger associated with connecting electricity illegally, tempering with government installed facilities, and acquire knowledge on how to save energy. With these, the proposed technique is feasible, workable, and implementable.

XI. THE PROPOSED STRUCTURE OF THE TECHNIQUE

Figure 4 shows the proposed structure of the technique and the interaction of the network elements.

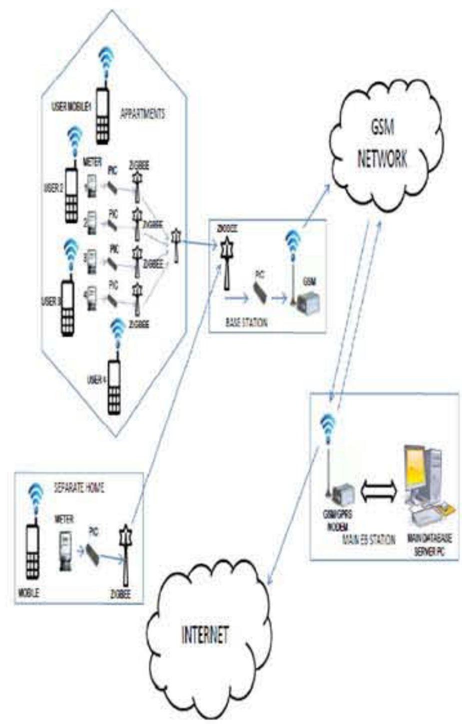

Fig. 4. Proposed Structure and Network Configuration

XII. CONCLUSION

Electricity theft is a growing problem nationally, and impoverished people tend to make a living out of it. Most fatalities occur in the informal settlement, and incidents are not reported to Law Enforcement. Electric cables lie across roads, railways, from one building to another in the formal places, from one tin house to another. Electricity theft can be classified as an electricity theft pandemic. In some communities, there are kingpins. These unscrupulous people build their own substation and supply to the community, at a fee every month. Imposing significant fines to them showed no good results because of the high unemployment rate. The culprits tend to reconnect themselves due to failure to afford to pay high penalties imposed on them and end up reconnecting themselves illegally. The research study proposes wireless techniques (ZigBee), taking cognizance of communication constraints over long distances. The ZigBee technique is a recommended technology solution that can mitigate electricity theft due to its characteristics of wireless and automated. It also comprises of star and mesh networks. It requires less staff, less management resulting in next to zero maintenance.

In this pilot study, the techniques show good results for the solution of curbing electricity theft, but like in any other procedure, advantages and disadvantages exist. A constraint with ZigBee technology is that in very long distances, it may have problems communicating clearly, 'The further you go, the lesser the communication". The causes being that, if long structures exist between router or radio or any other unforeseen interference, then highly possible such failure will be experienced. The solution for the problem is to mount the ZigBee on top pole boxes, meaning it can work better when installed in upper structures, communication can improve over a long distance. The problem of cyber-attack on the network may be resolved by the monitoring of the network, tracking every action that is taking place in your network, and placing a firewall into your head end system to protect the system from unauthorized exploitation of the system, network, and technologies.

REFERENCES

[1] T. B. Smith, "Electricity theft: a comparative analysis," *Energy policy*, vol. 32, no. 18, pp. 2067-2076, December 2004.

[2] I.E. Davidson, "Evaluation and effective management of non-technical losses in power networks," *The Transactions of the South African Institute of Electrical Engineers*, Vol. 94, No.3, Sep. 2003, pp. 39-42.

[3] D. Gerbec, S. Gasperic, I. Simon and F. Gubina, "An approach to customers daily load profile determination," IEEE Power Engineering Society Summer Meeting, pp.21-25, July 2002.

[4] A.H. Nizar, Z.Y. Dong and M. Jalaluddin, "Load profiling method in detecting non-technical loss activities in a power utility," IEEE Proceedings of the 1st International Power and Energy Conference on Computational Intelligence and Security, Heidelberg , Germany, pp.82-87, November 28-29, 2006.

[5] U. Hashmi and J.G. Priolkar, "Anti-theft energy metering for smart electrical distribution system," Proceedings of IEEE International Conference on Industrial Instrumentation and Control (ICIC), pp.1-5, 2015.

[6] J. Nagi, K. Yap, F. Nagi, S. Tiong, S. Koh, and S. Ahmed, "NTL detection of electricity theft and abnormalities for large power consumers in TNB Malaysia," in 2010 IEEE Student Conference on Research and Development (SCOReD), 2010, pp. 202-206.

[7] http://www.moneyweb.co.za/archive/eskom-customers-subsidise-huge-electricity-losses/ available on line, unpublished.

[8] P. Glauner, J. Meira, P. Valtcher, R. State and F. Bettinger, "The challenge of non-technical loss detection using artificial intelligence: A survey," International Journal of Computational Intelligence System, Vol.10, pp.760-775, 2 June 2016.

[9] F. Biscari, I. Monedero, C. Leon, J.I. Guerrero, J Biscari, and R. Millan, "A mining framework to detect non-technical losses in power Utilities," University of Seville Spain, ICEIS (2), pp.96-101, January 2009

[10] Ahmad T. Non-technical loss analysis and prevention using smart meters. Renewable and Sustainable Energy Reviews, Vol. 72, pp. 573-589, May 2017..

[11] J.E. Calmeyer, "The role of smart metering in revenue protection," The Electricity Regulations for Compulsory Norms and Standards for Reticulation Services of Electricity Regulations Act No.4 of 2006, Strike Technologies, pp.32-34, August 2011.

[12] V. Pandey, S. Gill and A. Sharma, "Wireless electricity theft detection system using ZigBee technology," Computing and Communication, Volume 1, Issue 4, pp.364-367, March 2013.

[13] X. Du and H. Chen, "Security in wireless sensor networks," in *IEEE Wireless Communications*, vol. 15, no. 4, pp. 60-66, Aug. 2008.

[14] V.C. Gungo and F.C. Lambert, "A survey on communication networks for electric system automation," *School of Electrical and Computer Engineering, Georgia Institution of Technology*, pp.1-5, unpublished.

[15] G. N. Ericsson, "Cyber security and power system communication—essential parts of a smart grid infrastructure," *IEEE Transaction on Power Delivery,* vol. 25, no. 3, pp. 1501-1507, 2010.