The Nucleus ***52****, No. 1 (2015) 40-44*

www.thenucleuspak.org.pk

The Nucleus

ISSN 0029-5698 (Print)

ISSN 2306-6539 (Online)

Hardware Module for the Security Enhancement of Optical Telecom Network Equipment

Nadeem* and M. Ali

Electrical Engineering Department, University of Engineering & Technology, Lahore, Pakistan

ARTICLE INFO

Article history :
Received : 18 December 2014
Revised : 23 February 2015
Accepted : 26 March 2015

Keywords :
OFAN
OLT
ONU
GSM

ABSTRACT

The telecommunication equipment physical security threats have increased not only in Pakistan but also anywhere in the world and hence, reducing the revenue. This new challenging and alarming situation is created for the telecom network provider. The main focus of this paper is to provide a low cost economical design for reducing the theft of the costly telecommunication equipment like optical network units (ONU). This system is based on instant messaging on the mobile in the event of theft through GSM modem. The proposed security module is dynamic, flexible and can also be integrated in the existing networks and separately having its own independent low power consumption source. The module will continuously work successfully under different scenarios such as completely isolated from other devices by power break down or by fibre cut.

I. Introduction

The speedy and terrific advancement in the field of telecommunication is exceptional from the last few decades which causing the sudden increasing outflow of both local as well as long distance interchanges of data. If the network facilitator continuously practiced in ordinary manner of delivering the service facility on the mode of copper wire system, then the demand of the corporate client for enormous amount of data will not be rewarded [1]. This situation alarmed and prepared the network service facilitators to groom up in new challenging time.

The emergence of optical fibre cable technology in early 1980 made a revolution in transmitting data [2][3].The huge demand of bandwidth is causing the replacement of old networks with the optical networks and providing maximum capacity to fulfill the demands of individuals and corporate customers. The deployment of the optical networks has increased the net profit value for the provider due to the reduction of the infrastructure and maintenance expenditures, but the security and safety of the optic fibre cable equipment mounted far away caused the security problem. One of the chief empires in telecommunication sector in Pakistan is Pakistan Telecommunication Company Limited (PTCL) which is delivering all types of telephonic, broadband and Internet services and covering wide range of area from urban to rural. The equipment are installed outdoor in mini exchanges and theft of the worthy equipment like batteries, controlling and services cards resulted in loss of billions of rupees. This problem arose due to lack of sufficient protection of the equipment.

For security purpose, following techniques are deployed for the equipments' safety.

1.1. Closed Circuit TV

The Close Circuitry Television (CCTV) networks for corporeal protection are being most widely used technologies. Internet based CCTV flourished in the society due to the expansion of the Internet [4]. The crime prevention is now regularly monitored and controlled by the use of CCTV.

The CCTV arrangement consists of supervision cameras, connected to a central server for image monitoring, as well as the client. The communication channel in the CCTV structure is either wire or wireless network for the monitoring of a particular location for security and analyzing the images.

The basic components for the formation CCTV are the inspection camera, image control server for image monitoring, access control server for identification, cell phone, desktop, and laptop.

1.2. Biometrics Techniques

The biometrics technique is a dominating technology that has been widely used for jail security, secured access control system and forensics [5]. The recognization of someone is primarily determined by the biological characteristic which is identified on the basis of some pattern recognition system and authentication is granted. For security purpose, biometric technology is used in an access control system. Human characteristics showing uniqueness in individual are deployed in latest biometric systems for identification. Some of these are :

- Pattern of vocal tract and voice
- Fingerprint

* Corresponding author : nadeemengineer@yahoo.com

- Hand geometry
- Retina of eye
- Marking sign

1.3. Door Sensors

The door sensors are also used for security applications [6] and when someone illegally enforced to open the door without prior intimation then alarms are generated for theft indication. The door sensors are easily installed and managed and can cope to some extent for security purpose.

1.4. Centralized Network Management System

The centralized network management system is also primarily used by the service provider for getting and monitoring of different alarms of equipment's and is the proprietary of vendors.

All the security techniques mentioned above are based on hardwired alarms system. These systems are deployed using wiring cables between alarm monitoring panels and devices. These systems cannot deliver instant messages in case of malicious activities to different locations. They are not flexible and are independent from each other. They provide alarms on certain fixed spots whereas the proposed new hardware module is low cost, dynamic and flexible and can deliver anywhere.The proposed security module based on GSM provides the excellent recompense of both hardwired and wireless alarm systems. It will not only ensure highest degree of secure and reliable performance, but also flexibility for setup and installation.The performance of the new module will be exceptional for greater control on safety and security. Physical security for the equipment will become easy, efficient and simple by the use of this new module.

The rest of the paper is divided into following sections: Section 2 describes the optical fibre access network (OFAN); Section 3 is about the design features of the hardware module; Section 4 presents the complete security module developed and Section 5 concludes the paper.

2. Optical Fibre Access Network (OFAN)

The types of access network that uses the optic light rays for reception and transmission of data by the induction of optical fibre technology is known as OFAN [7]. The overall bandwidth in the optical access networks increased up to several Giga bits per second (Gbps).The foremost components of the optical access system deployed by the PTCL are shown in Figure 1 and summarized below :

2.1. Optical Line Terminal (OLT) Unit

OLT is mounted at evidences of service provider. Examples of such places are the buildings of the telephone company or local area exchange, near the switching centre of a company and cable TV network provider ends. Various types of interfaces are available like E1/V5 interface that are used to attach the OLT and main telephone local exchange or digital distribution frame (DDF).

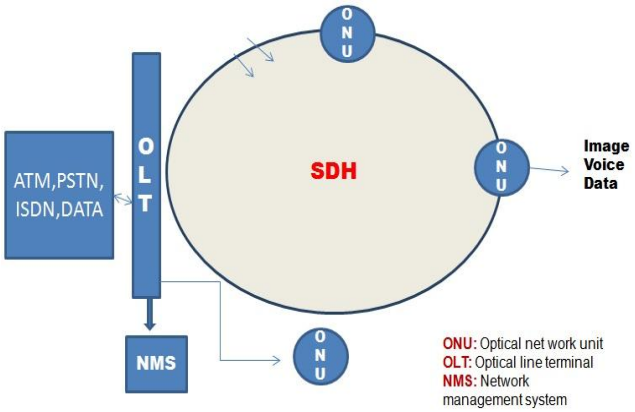

Fig. 1: Optical Fibre Access Network (OFAN)

The major functionalities of the OLT are described as [8]:

Interface establishment between optical network and ordinary network.

- OLT maintains the service quality
- Flexible and dynamic provision of allocation of bandwidth
- Different kind of alarms are generated for ONU's like fibre cut, failure of power and temperature reading etc.
- Different wavelengths for sending and receiving the data to and from the ONU's are also the core function which is provided by the OLT.

2.2. Optical Network Unit (ONU)

ONUs is installed at customer premises to execute the services to client, most probably neighborhood, within the office building, apartments or near residential home area [9][10]. The users of telephone, broadband services and smart TV etc., are connected to customer sides of ONU's directly by the drop wire or cable of twisted pair of different category to accomplish their demands.

As per planning and designing of the services and network, various hierarchies of structure of the ONU's formation in the geographical area can be employed like mesh topology, star, tree and ring, which provide the basis of communication between ONUs and OLT.

The transmission technology like Plesiochronous hierarchy, DWDM and SONET or SDH can be imposed for the communication in networking of the ONU typology [11]. The interfaces provided for the diversity of services by the ONU are mentioned below:

- Z interface is used for the services of plain old telephone customer

- The clients which require digital services like primary data rate of 30 channels and one channel for signaling and 2 channel for data and signal channel can use U interface
- N×64kbps can use V.24-V.35 interface to different subscribers
- Coaxial cable interface in the form of E1 are used for most common dedicated line of data rate of 2Mbps
- The CATV operators patch the signals via coaxial cable to CATV interface
- High date rate 10Mbps/100Mbps are provided by the FE interface

ONUs is under the constant risk of theft and controlling this security elapse is a big challenge for PTCL.

3. Design Features of the Security Module

This paper presents a low cost valuable hardware module for generating instant message in the event of theft. The principal design features of the security are summarized as :

- It is cheaper and flexible design as compared to the other market security system.
- The new security system can not only be installed in the present system but can also be used in all new incoming telecommunication equipment to improve safety.
- The system will be supportive under the situations when network managing system totally fails to deliver alarms at monitoring terminals of the fibre system due to power failure, fibre cable cut or some other malicious action.
- It is flexible and dynamic system.
- Operated on very low power for its all operation
- All types of alarms can be incorporated through instant messaging to any location

The proposed model shown in Fig. 2 consists of the following components :

- Detector circuits for the unauthorized removal of equipment.
- Microcontroller for controlling the operations.
- GSM module for interfacing and communicating theft messages to the concerned security personnel for preventing thefts of costly equipment.
- Mobile phone to which the theft message is sent.

The major hardware components for developing the security module are explained below :

3.1. 89C51 Microcontroller

The 89C51 is a CMOS 8 bit microcontroller used due to the following main characteristics:

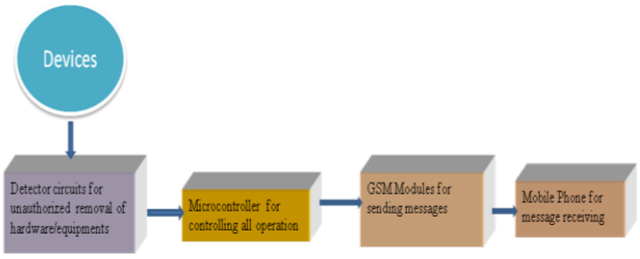

Fig. 2: Proposed model

- High performance and cost efficient solutions to many applications
- Easy availability
- Low power consumption
- Low price

3.2. GSM Module

A GSM modem is used in many commercial applications for sending and receiving messages through the modem interface. The module is used in this project is Sim900D shown in Fig. 3. It is manufactured by SIMCom. This module is operated in all frequency bands as a normal cell phone. Any network operator SIM card that supports GSM can be used in the module to establish a connection. The communication operation between the modem and PC is mainly controlled by AT commands. GSM modules can execute some extended commands set along with standard AT commands set.

Fig. 3: GSM Modem Sim900D

The AT commands are utilized for communication between the microcontroller and GSM modem by serial port for all the operation of security module. The theft alerts are sent through these AT commands to the modem for instant messaging. Some of the commonly used commands are mentioned in Table 1.

Table 1: AT Commands

Commands	Description
AT+CGMM	Model number finding
AT+CGMI	Name of manufacturer
AT+CGMR	Version of software
AT+CSQ	Radio signal strength
AT+CMGS	Sending data
AT+CMGR	Reading date

Following functions can be performed through these extended AT commands standard protocols [12, 13] :

- Messages can be read, written or deleted
- Text messages are sent
- Strength of signal can be visualized
- Battery charging status and level of charging can also be monitored

3.3. MAX232

MAX232 is popularly used integrated circuits for serial communication between any class of microcontrollers and computers (PC). In serial communication, it is utilized for converting the voltage from TTL/CMOS logic to RS232 logic levels. The voltage level of a microcontroller based on TTL (Transistor Transistor Logic) is between 0 to 5V whereas a PC voltage level varies between -25 to + 25V. Therefore, direct serial interfacing of microcontroller to PC is not possible and instead MAX232 is placed between them. In the design of security module, two MAX232 are used; one for communication with PC and the other for communication to the GSM modem.

4. Hardware Security Module

The interfacing of all components is shown in the schematic diagram in Fig. 4. The core part is 89C51 microcontroller in which the Hex file of C-program is burned for performing all security operation.

The complete hardware for the security protection is shown in Figure 5. The status of the hardware can be visualized with the help of different LEDs mounted on the board. LEDs give the indication of different types of communication and certain action or response by the microcontroller. Some of them represent the serial communication taking place between microcontroller and PC and other represent the instant message delivery status to the concerned security personnel through the GSM modem.

The optical networks units are installed at remote geographic area far away from the centre telecom office as shown in Figure 1. The proposed security module can be integrated with ONU.

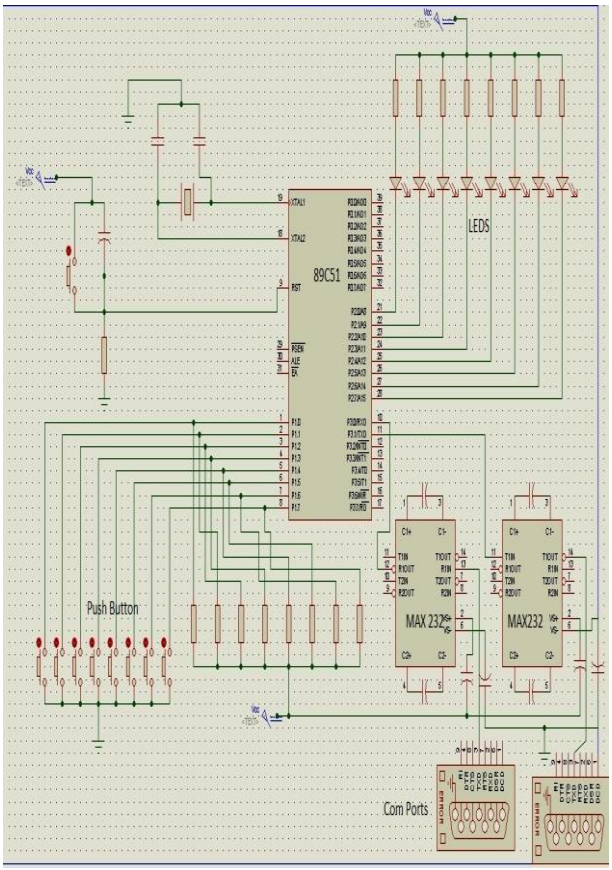

Fig. 4: Interfacing of different components

Initially two mechanisms are provided in the design module for providing security which shows its robustness to use it anywhere according to different circumstances, need and requirement.

4.1. Serial port

The serial port provided on the module can be connected to any device such as biometric system from which serial communication takes place and on the basis of communication instant messages are generated.

After completion of biometric process the result of known/unknown person is sent to the security module and it generates the theft message through GSM modem to the concerned security personnel to take preventive measures. The message is shown in Figure 6.

4.2. 8 Ports Switch

The option of single pole, double throw (SPDT) switches is also fabricated in the design and devices like cards, batteries etc., can also be connected through these switches. It can provide a mechanism of instant message generation on the activation of these switches. The malicious activities on costly equipment are reported in the form of SMS to mobile as shown in Figure 7.

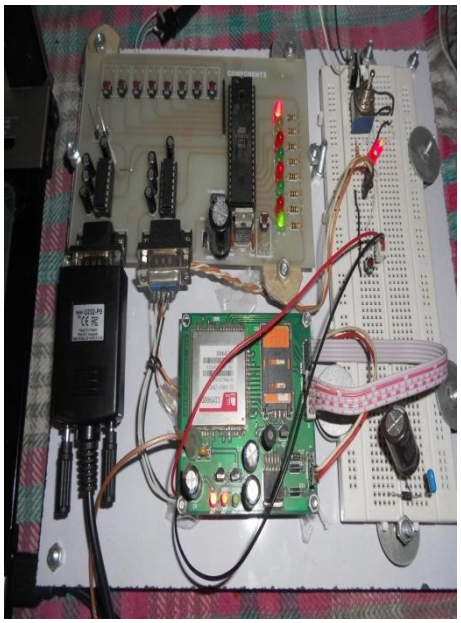

Fig. 5: Complete hardware module

Fig. 6: Security message in case of biometric process

Fig. 7: Security message in case of SPDT switches

5. Conclusion

A better security system in telecom networks is the output of this research work, based on alarms generating design for minimizing the risk in security of network equipment. The new security provision will reduce the response time in the event of theft and elevate performance of the service provider and eventually the profit. A hybrid model is implemented to integrate wireless communication in an optical network, which can send instant messages regarding the theft of ONUs, when the system is cut off completely from the central monitoring system and having no way to generate the alarms for monitoring purpose.

References

[1] ITU-T Rec. G.902, "Framework recommendation on Functional Access Networks, Architectures and Function, Access Types, Management and Service Node Aspects", November, 1995.

[2] Y. Su, "All-optical virtual-private-network in access networks" in *Proc. LEOS*, 2007, pp. 802–803.

[3] J. J. Koponen and M. J. Soderlund, "A duplex WDM passive optical network with 1:16 power split using reflective SOA remodulator at ONU" in *OFC 2004*, Los Angeles, CA, 2004.

[4] Han Byoung-Jin and Hyuncheol Jeong, "The privacy protection framework for biometric information in network based CCTV Environment", IEEE Conference on Open Systems (ICOS2011), September 25–28, 2011, Langkawi, Malaysia.

[5] Biometrics (Fingerprint Sensor) on http://www.atmel.com/ products/ Biometrics/ , 2007-04-10

[6] S. S. S. Ranjit, A. F. Tuani Ibrahim, S. I MD Salim and Y. C. Wong, "Door Sensors for Automatic Light Switching System", Faculty of Electronics Engineering and Computer Engineering, University Teknikal Malaysia Melaka (UTeM) Durian Tunggal, Malaysia.

[7] D.B. Payne and R.P. Davey: A new architecture for optical networks. Telektronik, 2005.

[8] Dong-Becom Shin et al., "An ONU Design for EPON-based Access Network" The 9th APCC, Penang, Malaysia, 21-24 September, 2003.

[9] G. Kramer, "The problem of upstream traffic synchronization in Passive Optical Networks" Davis, CA 95616.

[10] Y. Chen, W. Tang, "Concurrent DWDM Multi-Mode Switching: Architecture and Research Directions," IEEE Communications Magazine, vol. 48, no. 5, May 2010.

[11] Soo-Jin Parket. al., "Fibre-to-the-Home Services Based onWavelength-Division-Multiplexing Passive Optical Network" IEEE Journal of Lightwave Technology, vol. 22(11), November 2004.

[12] Y. P. Tsou, J. W. Hsieh, C. T. Lin, and C. Y. Chen, "Buliding a remotesupervisory control network system for smart home applications," IEEE International Conf. on System, Man andCybernetics, pp. 1826-1830, 8-11 October, 2006.

[13] B. Yusekkaya, A. A. Kayalar, M. B. Tosun, M. K. Ozcan, and A.Alkar, "A GSM, internet and speech controlled wireless Interactive Home automation system," IEEE Transaction on ConsumerElectronics,vol.52 no. 3, pp. 837-843, Aug. 2006.